拓林思（中国）软件有限公司

GreatTurbo Enterprise Server 10

Powerful Thinking.

用户指南

中国北京市朝阳区建国门外大街甲 12 号 • 新华保险大厦 5 层 503 室
电话 +86 010 65054020 • 传真 +86 010 65054017 邮编 100022

目　　录

▪ 前 言



本手册由 Turbolinux Inc. 设计和完成。

联系方式：

电 话： 86.10.65054020

传 真： 86.10.65054017

地址： 北京朝阳区建国门外大街甲 12 号 新华保险大厦 5 层 503 室

邮政编码： 100022

网址： http://www.turbolinux.com.cn/

1.1 致谢

GreatTurbo Enterprise Server 10 用户指南提供关于使用 GreatTurbo Enterprise Server 10 所需要的所有信息，该 GreatTurbo Enterprise Server 10 采用 Linux 2.6.9 内核, 部分汉字字库采用东文字库。

感谢您从众多的 Linux 中选择 Turbolinux!

在中国、美国、日本 Turbolinux 公司的共同努力协作开发下 Turbolinux 具有安装简便、应用广泛、性能高、便于使用的特点。

自 1993 年以来，我们一直进行 Linux 方面的工作，Turbolinux 在太平洋沿岸地区是 Linux 的带头羊。我们在 1997 年就推出了自己的国际化版本，目前支持简体中文，繁体中文、日文、韩文以及英文。有关 Turbolinux 的最新信息，请访问我们的 Web 站点 http://www.Turbolinux.com.cn/。

通过开放源码运动以及 Linux 的缔造者 Linus Torvalds 的推动，我们的事业取得了成功：通过我们的共同努力，用户对 Turbolinux 感到满意。我们向那些已经而且继续为实现这一目标作出贡献的Linus Torvalds 以及世界各地无数的 Linux 开发者们表示感谢。

1.2 印刷规范

本指南使用以下规范：

- 文本中的英文字符表示以下情况：
  - 变量名，目录名，文件名
  - 命令，选项，参数以及用户输入
  - URL (Web 站点名)
  - email 地址
  - 被强调的字(第一次出现)
- 文本中的用引号括起的内容表示屏幕名
- 文本中的用引号括起的英文内容表示命令，程序，出现在 GUI 上的按钮，

菜单项，选项

• 以灰色背景显示的文本表示用户在终端屏幕上输入的命令行或屏幕文本。

• 斜黑体单间隔(Courier)字符表示用户输入的字符串的名称。例如，password 意思为用户输入自己的密码，而不是字符串“pasword”这个字本身。

• 出现在系统响应中的用角括弧“ <>”括起来的常规非黑体单间隔字符表示字符串的名称，该字符串被系统用实际的字符串替换。例如，<host_address>可以被显示为 192.168.1.10。

• “讯息字符串”由双引号（“”)括起来。

• GreatTurbo Enterprise Server 10 缩略写作 GTES10 ，以下的缩写 GTES10 代替的是 GreatTurbo Enterprise Server 10。

1.3 征求用户反馈

Turbolinux, Inc. 坚持不懈地努力优化和改进自己的产品，我们极为重视用户的反馈和意见，欢迎用户指正出现的任何失误、不足、错误或遗漏。用户的需求、意见和建议是我们在下一个版本中进行改进和提高的依据。

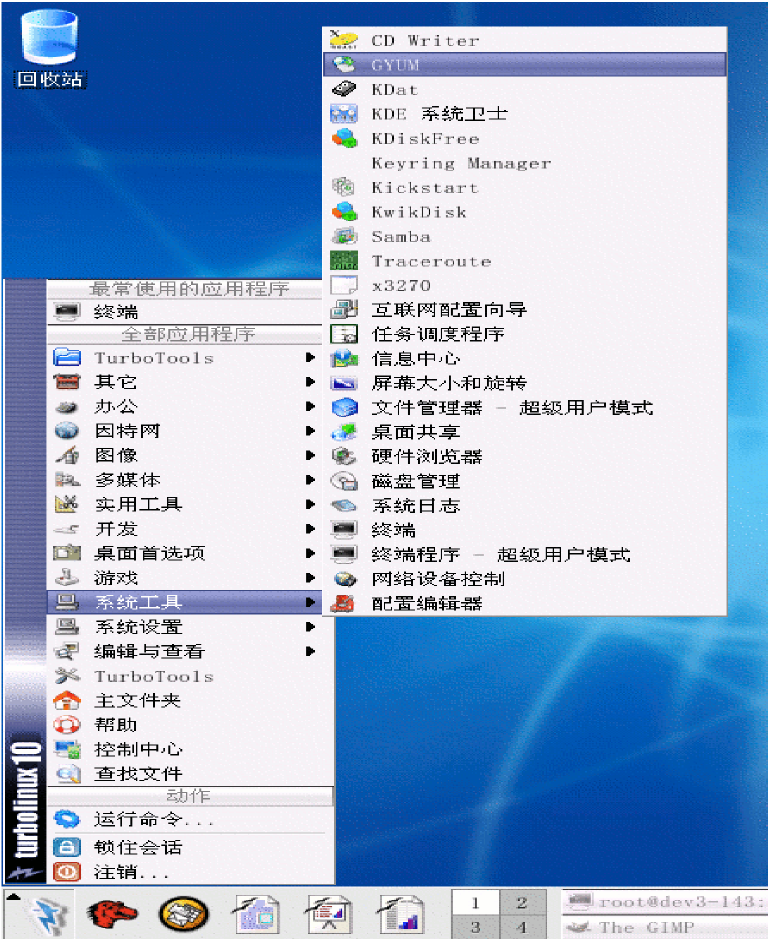
如果您对我们的产品何方面有什么意见和建议，请告知我们。我们静候用户的心声。我们的 Email 为 support@Turbolinux.com.cn .

1.4 技术支持

Turbolinux 向购买我们光盘的用户提供各种形式的技术支持。详情请参观我们的 web 站点 http://www.Turbolinux.com.cn/， 获取技术支持前请务必登记你的 Turbolinux 产品，以便获得这些支持。登记时，需要产品注册号码，该号码在 GreatTurbo Enterprise Server 10 包装盒中。

1.5 在线更新

GreatTurbo Enterprise Server 10 具有多种升级手段，其中，方便快捷的在线更新为用户提供了更加灵活的升级方法。在安装完毕的系统中，按照图中所示，选择 Turbo 在线升级。



出现使用界面后，就可以进行“安装”、“删除”、“升级”等操作。因为连接数量有限，如果运行失败，请多尝试几次。也可以选取“设置”来设置升级服务器的地址信息。

1.6 Service Pack 功能

Turbolinux 公司始终致力于保持产品与业界最新，最成熟技术的同步性。除了多种更新手段以外，还提供定期的 Service Pack。Service Pack 将是对一定时期内系统更新的一个总结。当新的 Service Pack 盘出现的时候，用户进行系统安装就应该选择 Service Pack 盘作为第一张安装盘，然后按照相关安装步骤进行安装，在全部系统安装完毕以后，安装系统会提示再一次插入 Service Pack 盘。当上述所有的步骤都完成的时候，系统就已经是经过升级后的系统了。

第一章　GTES10 系统特性

1.1 GTES10 发行版简介

1.1.1 SELinux 的实现

GTES10 包括了一个 SELinux 的实现。SELinux 代表了用户，程序以及进程间相互交流的主要变化。在这个发行版本中，SELinux 被默认安装并被开启使用。在安装的过程中，您可以选择禁用 SELinux，或是设置它只记录警告信息，或是使用它的只在以下守护进程中有效的目标化策略：dhcpd、httpd、mysqld、named、nscd、ntpd、portmap、postgres、snmpd、squid、syslogd。目标化策略在默认的情况下被启用。

1.1.2 挂载 NFS 时 mount 命令已被改变

TCP 是 NFS 挂载时的默认传输协议。这就意味着 mount 命令不再使用 UDP （例如，mount foo:/bar /mnt），而是使用 TCP 来与服务器进行通信。

1.1.3 包含了 Subversion 1.1

Subversion 1.1 现在被包括在 GTES10 中，Subversion 版本控制系统是被用来替代 CVS 的。它提供了 atomic commits，文件，目录和元数据 (metadata) 的版本控制等新功能以及 CVS 所提供的大部分功能。

1.1.4 包含了 ACPI 的支持

GTES10 现在包括对 Advanced Configuration and Power Interface (ACPI) 的支持。ACPI 是一个被大多数新硬件支持的通用的电源管理技术规格。

1.2 软件包相关的注记

1.2.1 基本

本节包含了关于基本系统组件的信息。

1.2.1.1 openssh

GTES10 提供了 OpenSSH 3.9。OpenSSH 3.9 包括了对 ~/.ssh/config 文件的严格的权限和所有者权限的检查。这些检查使得当这个文件没有适当的所有者权限和访问权限时，ssh 会退出。

1.2.2 核心

1.2.2.1 e2fsprogs

ext2online 工具被添加用来在线地扩大已存在的 ext3 文件系统。需要注意的是，ext2online 并不能扩大它所在的块设备本身 — 一定要有足够的未被使用的空间在这个设备上。最简单的方法是使用 LVM 卷并运行 lvresize 或 lvextend 来扩展这个设备。另外，文件系统一定要在实际改变大小之前做好准备。这些准备包括，为 on-disk 分区表的增加保留一个小的空间。对于新建的文件系统， mke2fs 会自动保留这样的空间。这个保留的空间应该足够文件系统增加 1000。如下命令可以禁用建立保留空间的功能：mke2fs -O ^resize_inode。

1.2.2.2 glibc

GTES10 提供的 glibc 可以执行附加的内部数据健全检查，从而在尽可能早的时候发现和保护数据被破坏。在默认的情况下，当被破坏的数据被发现时，与以下相似的错误信息会被显示在标准的错误输出上（如果 stderr

没有打开，会被记录在 syslog 中）：

*** glibc detected *** double free or corruption: 0x0937d008 ***

在默认的情况下，产生这个错误的程序也会被中止。但是，这（以及是否产生错误信息）可以通过环境变量 MALLOC_CHECK_ 来控制。以下的设置是被支持的：

- 0 — 不产生错误信息，也不中止这个程序
- 1 — 产生错误信息，但是不中止这个程序
- 2 — 不产生错误信息，但是中止这个程序
- 3 — 产生错误信息，并中止这个程序

如果您的由第三方 ISV 提供的程序会引发这些数据破坏检查并显示错误信息，您应该向这个程序的提供者提交一个错误报告，因为它代表了一个严重的错误。

注意：如果 MALLOC_CHECK_ 被设置为除 0 以外的值，这会使 glibc 进行更多的检查并可能影响到系统的性能。

1.2.3 内核

本节涉及与 GTES10 内核相关的问题。

1.2.3.1 hugemem 新内核

GTES10 包括一个叫做 hugemem 的新内核。这个内核支持每进程 4GB 用户空间（其它内核只支持 3GB）和 4GB 直接内核空间。使用这个内核允许 GTES10 在拥有大至 64GB 主内存的系统上运行。一般来说，配置了 16GB 内存以上的系统需要 hugemem。使用较少内存的环境也可以从这个内核中获益，特别是在运行能够从较大的用户空间中获益的应用程序的时候。注意：要为内核和用户空间提供 4GB 地址空间，内核中必须保持两个分开的虚拟地址映射图。这会给用户和内核空间的转换带来些额外的系统开销，例如在系统调用和中断的时候。这些额外的系统开销对整体

性能的影响在很大程度上要依据应用程序而定。如果您要安装 hugemem 内核，在引导提示后键入以下命令：

```
rpm -ivh <kernel-rpm>
```

这里的 <kernel-rpm> 是 hugemem 内核 RPM 文件的名称 —例如，kernel-hugemem-2.6.9-1.i686.rpm

安装完成后，重新引导您的系统，请确定选择新安装的 hugemem 内核。测试了这个使用 hugemem 内核的系统能够正确运行后，您应该修改 /boot/grub/grub.conf 文件来默认引导 hugemem 内核。

1.2.3.2 rawio

虽然 GTES10 包括对 rawio 的支持，但它已是一个过时的接口。如果您的应用程序使用这种接口，我们建议您改变您的应用程序，使它们通过 O_DIRECT 标志来打开块设备。

1.2.3.3 声音子系统

现在的声音子系统是基于 ALSA 的，OSS 模块已不再有效。

1.2.3.4 增强磁盘设备

GTES10 提供的内核包括了对增强磁盘设备 - Enhanced Disk Device (EDD) 的支持。增强磁盘设备是直接从磁盘控制器 BIOS 中查询可启动磁盘设备的信息，并把它存储为 /sys 文件系统中的一个记录项。两个与 EDD 相关的重要的内核命令行选项已被添加：

- edd=skipmbr — 当有其它调用在从磁盘控制器查询信息时，禁用对磁盘读的 BIOS 调用。当系统 BIOS 报告的磁盘数量多于实际系统中的磁盘数量时，可以使用这个选项。这将会导致在加载内核时的一个 15 到 30 秒的延迟。
- edd=off — 禁用所有与 EDD 相关的对磁盘控制器 BIOS 的调用。

1.2.3.5 USB 存储设备

虽然 GTES10 的初始发行版本不支持 USB 硬盘设备，但是其它的 USB 存储设备（如闪存介质，CD-ROM 和 DVD-ROM 设备）当前被支持。

1.2.3.6 megaraid_mbox 驱动

GTES10 所带的内核包括了由 LSI Logic 提供的 megaraid_mbox 驱动。这个驱动是替代 megaraid 驱动的。megaraid_mbox 驱动有一个设计方面的改进，它与 2.6 内核相兼容并包括对最新硬件的支持。但是，megaraid_mbox 不支持一些被 megaraid 驱动支持的老的硬件设备。megaraid_mbox 驱动不支持具有以下 PCI 厂商 ID 和 设备 ID 的试配器：

```
vendor, device

0x101E, 0x9010

0x101E, 0x9060

0x8086, 0x1960
```

lspci -n 命令可以被用来显示一台特定机器上所安装的试配器 ID。具有这些 ID 的产品型号名是（但并不只限于这些型号）：

- Dell PERC (dual-channel fast/wide SCSI) RAID 控制器
- Dell PERC2/SC (single-channel Ultra SCSI) RAID 控制器
- Dell PERC2/DC (dual-channel Ultra SCSI) RAID 控制器
- Dell CERC (four-channel ATA/100) RAID 控制器
- MegaRAID 428
- MegaRAID 466
- MegaRAID Express 500
- HP NetRAID 3Si 和 1M

Dell 和 LSI Logic 已经声明他们不再在 2.6 内核中支持这些设备。因此，GTES10 不提供对这些试配器的支持。

1.2.3.7 iSCSI 软件

GTES10 的初始发行版本不包括对 iSCSI 软件 initiator 或 target 的支持。对 iSCSI 的支持正处于测试阶段，测试的结果将决定对 iSCSI 的支持是否会被包括在以后的 GTES10 升级产品中。

1.2.3.8 Emulex LightPulse 光纤通道驱动器

Emulex LightPulse 光纤通道驱动器 (lpfc) 正在被测试是否可能被包括在 Linux 2.6 内核中。它被包括在 GTES10 中用于测试的目的。这个驱动程序很可能被修改。如果这个驱动程序有问题，或是它将不再包括在 Linux 2.6 内核中，最终的 GTES10 发行版本可能将不提供这个驱动程序。

lpfc 驱动程序有如下的已知错误：

- 当短期的 cable pull, 交换机重启或是设备消失的时候，驱动程序不会隔离系统。因此，系统可能会过早地认为一个设备已不存在而把它离线。在这种情况下,手工地重新激活这个设备从而使系统可以使用它是需要的。
- 当这个驱动程序被 insmod 插入时，如果按 Ctrl-C 可能会导致错误。
- 在 insmod 仍在运行时运行 rmmod 可能会导致错误。
- 为了使 SCSI 子系统可以检测到这个新设备，它的插入需要被手工地搜索。

1.2.3.9 升级内核

过去，升级内核的过程不会改变系统的启动装载配置中的默认内核。GTES10 改变了这种情况。它把最新安装的内核设置为默认的内核。这种情况在所有的安装方法中都有效（包括 rpm -i）这个行为被 /etc/sysconfig/kernel 文件中的两行所控制：

- UPGRADEDEFAULT — 控制新内核是否在默认的情况下被启动 （默认值： yes）
- DEFAULTKERNEL — 名为这个值的内核 PRM 将在默认的情况下启动（默认值：取决于硬件的配置）

1.2.4 sysklogd

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.5 DNS 域名服务器

本节包含关于 DNS 名称服务器的信息。

1.2.5.1 bind

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.6 开发工具

本节包含关于核心开发工具的信息。

1.2.6.1 memprof

由于和当前版本的 C 语言库和工具链不能正确地在一起工作， memprof 内存档案和泄漏检查工具不再包括在 GTES10 中。memcheck 和 massif 以插件的形式出现在 valgrind 中。

1.2.7 图形化互联网

本节包括了帮助您浏览互联网的软件包，包括图形化的电子邮件，万维网浏览器和聊天室。

1.2.7.1 evolution

GTES10 提供了一个升级的图形化的 Evolution 电子邮件客户端程序。这个新版本增加了一些新功能，包括：

- 新版的 Evolution 包括了一个具有学习功能的垃圾邮件过滤器。这个过滤器可以更有效地区分垃圾邮件和非垃圾邮件。当您收到垃圾邮件，点击 Junk 按钮。定期查看您的垃圾邮件目录，检查其中是否有被错误地当成垃圾邮件的非垃圾邮件。如果有，把它们标记为 Not Junk。通过这些行动，垃圾邮件过滤器就会逐渐变得非常的有效。
- Evolution Connector 可以使您与 Microsoft Exchange 2000 和 2003 服务器连接。
- 用户界面已被大大改进，每一种操作（电子邮件，日历，任务和联系人）都被分开处理，改变了以前以服务器为中心的形式。
- Evolution 提供了增强的加密和数字签名的功能，包括使用 S/MIME。
- Evolution 通过把它的设置文件名从 ~/evolution/ 改为 ~/.evolution/，达到对最终用户隐藏这个文件的目的。

1.2.8 图形

本节包括了帮助你处理和扫描图像的软件包。

1.2.8.1 gimp

因为 GIMP 已经被升级到 2.0，Perl bindings 已不再是主软件包的一部分， gimp-perl 不再被包括在 GTES10 中。

在 GIMP 中使用 Perl 脚本的用户应该从 http://www.gimp.org/downloads/ 上得到 Gimp Perl 模块并安装。

1.2.9 邮件服务器

本节包含关于 GTES10 提供的邮件传输代理的信息。

1.2.9.1 mailman

较早的 mailman RPMs 在 /var/mailman/ 的目录下安装所有的文件。不幸的是，这与 Filesystem Hierarchy Standard (FHS) 不一致，而且在 SELinux 启动时会破坏安全性。

如果您在以前安装了 mailman 并编辑了 /var/mailman/中的文件（如 mm_cfg.py），您必须按照如下的方法把这些改变存到新的位置：

```
/usr/share/doc/mailman-*/INSTALL.TURBOLINUX
```

1.2.9.2 sendmail

默认情况下，Sendmail 邮件传输代理（MTA）不接受来自本地计算机以外的主机的网络连接。如果您想把 Sendmail 配置成其它客户的服务器，请编辑 /etc/mail/sendmail.mc，并把 DAEMON_OPTIONS 行改变成监听网络设备（或者使用 dnl 来注释掉该选项）。然后您必须运行下面的命令（以根身份）来重新生成 /etc/mail/sendmail.cf：

```
make –C /etc/mail
```

注意，您必须安装了 sendmail-cf 软件包才能使上面的命令奏效。不正确的 Sendmail 配置可能会被当做开放的 SMTP 转发服务器使用。

1.2.10 MySQL 服务器

MySQL（多用户，多线程的客户机 / 服务器数据库）已经升级到版本 4.1.x。新版本的 MySQL 具有以下在速度，功能及可用性方面的改进：

- 子查询 (subquery) 的支持
- 非结构化查询的 BTREE 索引
- 使用 SSL 连接的安全数据库复制
- 通过使用 utf-8 和 ucs-2 字符集的 Unicode 支持

用户应该注意，当把 MySQL 升级到 4.1.x 版时，应用程序和数据库可能会出现兼容性的问题。一个已知的问题是默认的时间戳会改变。为了解决这个问题， mysqlclient10 软件包被提供。这个软件包用来为 3.23.x 客户端库 (libmysqlclient.so.10) 提供一个和与它们相连的应用程序的二进制兼容。虽然 mysqlclient10 软件包提供了对 MySQL 4.1.x 服务器兼容性的支持，但它不支持 MySQL 4.1.x 引进的新的口令加密方法。为了与老的 MySQL 3.x 客户程序兼容，/etc/my.cnf 配置文件中的 old_passwords 参数在默认的情况下开启。如果不需要与老版本客户程序的兼容，可以通过禁用这个参数来改进口令加密的方法。

1.2.10.1 mysql-server

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.11 网络服务器

本节包含不同的基于网络的服务器信息。

1.2.11.1 dhcp

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.12 服务器设置工具

本节包含关于不同服务器设置工具的信息。

1.2.12.1 system-config-lvm

GTES10 提供了一个图形化的 Logical Volume Manager (LVM) 配置工具 - system-config-lvm。system-config-lvm 允许用户为本地的物理磁盘和磁盘分区建立卷组群。它使得被创建的逻辑卷非常灵活，可扩展，并可以让系统象使用普通的物理磁盘一样使用这个逻辑卷。

system-config-lvm 使用图形来代表系统的磁盘和卷。这可以帮助用户更直观地查看存储设备的使用情况并为卷的管理任务提供了一个界面。

1.2.12.2 system-config-securitylevel

被 system-config-securitylevel 配置工具建立的防火墙现在允许 CUPS 和 Multicast DNS (mDNS) 浏览。请注意，当前这些服务还不能使用 system-config-securitylevel 来禁用。

1.2.13 万维网服务器

本节包含用于万维网服务器环境中的软件的信息。

1.2.13.1 httpd

在默认的 SELinux 安全配置中，httpd 被 targeted 策略所控制。它通过设定允许或拒绝 httpd 对系统的访问来增加系统的安全性和万维网服务器的稳定性。但是，这可能导致以前可以正常工作的配置（例如使用 PHP）不再可以正常工作，您应该了解 SELinux 的工作原理来保证您的系统即安全又可以正常运行。

例如，通过设置一个布尔值来为 httpd 设置权限， httpd 就可以读取在 ~/public_html/ 中被标记为 httpd_sys_content_t 的项。Apache 守护进程不能访问那些没有被 SELinux 设定可以被 httpd 访问的项（文件，应用程序，设备和其它进程）。

通过设置只允许 Apache 访问它所需要的功能，系统可以避免被破坏或错误的 httpd 守护进程配置。

因为需要使用标准的 Linux 和 SELinux 的文件和目录权限，管理员和用户需要了解重新标记的文件。重新标记包括以下命令（一个是重新标记目录的内容，一个是重新标记一个单一的文件）：

```
chcon -R -h -t httpd_sys_content_t public_html

chcon -t httpd_sys_content_t public_html/index.html
```

如果一个文件或目录没有被标记为在 Apache 允许类型的列表中的类型时，将会产生一个 403 Forbidden 错误。

您可以使用 system-config-securitylevel 来设置布尔值或是禁用控制 Apache （或任何守护进程）的目标策略。在 SELinux 页中的 Modify SELinux Policy 中，您可以为 Apache 修改布尔值。如果需要，您可以选择 Disable SELinux protection for httpd daemon 来禁止 unconfined_t 到特定守护进程的转换，如 httpd_t。禁用这个转换将关闭 SELinux 对这个守护进程的管理，使它只具有标准的 Linux 安全性。

在默认的情况下，httpd 守护进程使用 C locale，而不是使用被设置的系统的 locale。这可以通过修改 /etc/sysconfig/httpd 文件中的 HTTPD_LANG 变量来改变。

1.2.13.2 php

默认的 /etc/php.ini 配置文件已经把过去使用的默认值 "development" 改为使用 "production" 为默认值。不同的地方是：

- display_errors 现在是关
- log_errors 现在是开
- magic_quotes_gpc 现在是关

这个软件包现在使用 "apache2handler" SAPI 与 Apache httpd 2.0 集成，而不是使用 "apache2filter" SAPI。如果从以前的发行版本升级，SetOutputFilter 会被从 /etc/httpd/conf.d/php.conf 文件中删除。

PHP 扩展模块软件包有以下变化：

- gd, mbstring 和 ncurses 扩展已经被分别移到了 php-gd, php-mbstring 和 php-ncurses 软件包中。如果您是从以前的版本升级的，您需要手动安装这些软件包。
- domxml, snmp 和 xmlrpc 扩展现在分别在 php-domxml, php-snmp 和 php-xmlrpc 软件包中。

1.2.13.3 squid

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.14 X 窗口系统

本节包含 GTES10 提供的 X 窗口系统实现的信息。

1.2.14.1 xorg-x11

- GTES10 包括新的 xorg-x11-deprecated-libs 软件包。这个软件包包括了 X11 相关的库函数。这些库函数已经过时。为了使第三方的软件提供者可以有足够的时间来把使用这些库函数的应用程序进行修改，与这些程序二进制兼容的应用还被在这个版本中所维护。当前，这个软件包包括 Xprint 库函数 (libXp)。新的应用程序不应该再使用这个库。当前在使用这个库的应用程序应该升级到使用支持 libgnomeprint/libgnomeprintui 打印的 APIs.

- 用户对当 GTES10 X 窗口系统中与字体相关的问题可能会有一些混淆。当前，存在两个字体子系统，它们具有不同的特性：

- "核心 X 字体子系统" 是原始的（多于 15 年）子系统。被这个子系统处理的字体不是抗锯齿的。它被 X 服务器所处理，名字类似：

```
-misc-fixed-medium-r-normal--10-100-75-75-c-60-iso8859-1
```

新的字体子系统被称为“fontconfig”。它允许应用程序直接使用字体文件。fontconfig 经常与“Xft”库一起使用，这会允许应用程序在屏幕上绘制平滑字体。fontconfig 使用的名称更有“人情味儿”，它们类似：

```
Luxi Sans-10
```

随着时间的推移，fontconfig/Xft 将会取代核心 X 字体子系统。目前，使用 Qt 3 或 GTK 2 工具包（包括 KDE 和 GNOME 应用程序）的应用程序使用 fontconfig 和 Xft 字体子系统；其它程序多数使用核心 X 字体。注意：以上列出的字体子系统的使用有一个例外：OpenOffice.org 使用它自己的字体绘制技术。如果您想给您的 GTES10 系统添加新字体，根据使用新字体的字体子系统而定，您必须明确所需步骤。对于核心 X 字体子系统，您必须：

第 1 步 创建 /usr/share/fonts/local/ 目录（如果它不存在）：

```
mkdir /usr/share/fonts/local/
```

第 2 步 把新字体文件复制到 /usr/share/fonts/local/ 中

第 3 步 使用以下命令来更新字体信息（注意，由于格式限制，以下行并不以一行形式出现，但是在实际使用中，它应该在一行内输入）：

```
ttmkfdir -d /usr/share/fonts/local/ -o /usr/share/fonts/local/fonts.scale

mkfontdir /usr/share/fonts/local/
```

第 4 步 如果您必须要创建 /usr/share/fonts/local/，您就必须把它添加到 X 字体服务器（xfs）的路径中：

```
chkfontpath --add /usr/share/fonts/local/
```

把新字体添加到 fontconfig 字体子系统比较简单明了；只需把新字体复制到 /usr/share/fonts/ 目录中即可（个体用户可以把新字体复制到 ~/.fonts/ 目录中来修改他们的个人字体配置）。复制了新字体后，使用 fc-cache 来更新字体信息缓存：

```
fc-cache <directory>
```

这里的 <directory> 应该是 /usr/share/fonts/ 或 ~/.fonts/ 目录。个体用户还可以图形化地安装字体。方法是：在 Nautilus 中浏览 fonts:///，然后把新字体文件拖放到那里。注意：如果字体文件名以".gz"结尾，这表明它使用 gzip 被压缩，因而必须使用 gunzip 来解压后，fontconfig 字体子系统才能使用这个字体。

- 鉴于向基于 fontconfig/Xft 的新字体系统的转换，GTK+ 1.2 应用程序将不会被"字体首选项"对话框中做出的改变所影响。对于这些应用程序，字体可以通过在 ~/.gtkrc.mine 文件中添加以下几行来配置：

```
style "user-font" {

fontset = "<font-specification>"

}

widget_class "*" style "user-font"
```

（这里的 <font-specification> 代表被传统的应用程序使用的字体规定，如

“-adobe-helvetica-medium-r-normal--*-120-*-*-*-*-*-*”。）

1.2.15 其他

本节包含关于不属于以前介绍的任何类别的软件包的信息。

1.2.15.1 compat-db

C++ 和 TCL 绑定库不再包含在 compat-db 软件包中。需要使用这些绑定的应用程序必须指向当前的 DB 库。

1.2.15.2 lvm2

本节包含 lvm2 软件包的信息。

一个完整的 LVM2 命令被安装在 /usr/sbin/。在 /usr/ 还无效的启动环境中，每个命令前需要加上 /sbin/lvm.static（例如， /sbin/lvm.static vgchange -ay）。

在 /usr/ 有效的环境中，不再需要在每个命令前加 lvm （例如，/usr/sbin/lvm vgchange -ay 变为 /usr/sbin/vgchange -ay）。

新的 LVM2 命令（例如，/usr/sbin/vgchange -ay 和 /sbin/lvm.static vgchange -ay）会检测您是否在运行 2.4 内核。如果是，它会调用旧的 LVM1 命令。LVM1 已经被改为以 ".lvm1" 结尾（例如，/sbin/vgchange.lvm1 -ay）。

1.2.15.3 Net-snmp

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.15.4 Nscd

nscd 名称服务缓冲存储守护程序会在系统重新启动时保存它的缓存内容。每个数据库（用户，组群和主机）可以通过把 /etc/nscd.conf 文件中相应的行设为 "yes" 来实现这个功能。缓冲存储中的每条记录都将不会被删除，直到它们不再被需要。那些存活周期（time-to-live) 已经过期但是可能还会被使用的记录会被自动地重新载入。这在目录和名称服务暂时无效的时候非常有用。

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.15.5 Ntp

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.15.6 Portmap

在默认的 SELinux 安全配置中，这个守护进程是被 targeted 策略所规定的。它通过设定这个守护进程所需使用的系统目标的访问权限来提高系统的安全性。但是，这可能导致您以前可以运行的配置不再能够正常地工作。您必须对 SELinux 有足够的了解，从而达到可以使您的系统正常运行，又可以提高您系统安全性的目的。

1.2.15.7 udev

GTES10 不再象过去的版本那样，通过一个静态的 /dev/ 目录管理设备。

它通过 udev 动态地管理设备。它允许在驱动程序被加载时才按需创建设备节点。

关于 udev 的附加信息，请参阅 udev(8) 的说明书页。

udev 的额外的规则必须被存放在一个位于 /etc/udev/rules.d/ 目录中的单独文件中。

udev 的额外的权限规则必须被存放在一个位于 /etc/udev/permissions.d/ 目录中的单独文件中。

把系统升级到 GTES10 会被自动地重新配置使用 udev。但是（虽然不推荐），可以使用如下步骤来升级到 udev：

第 1 步 确定您正在运行 2.6 内核

第 2 步 确定 /sys/ 已被挂载

第 3 步 安装 GTES10 提供的 initscripts RPM

第 4 步 安装 GTES10 提供的新的 udev RPM

第 5 步 执行 /sbin/start_udev

第 6 步 安装 GTES10 提供的新的 mkinitrd RPM

第 7 步 执行以下的步骤之一：安装 GTES10 提供的新的 kernel RPM 或为您已存在的内核重新运行 mkinitrd

第二章　GTES10 系统使用

2.1　出发

2.1.1　安装向导（setup agent）

此部分对应 first boot，GTES10 中无 first boot。

2.1.2　术语介绍

用户在使用一个新的操作系统之前应该了解一下该系统的新术语。这一部分定义了一些用户应该了解的基本术语。

- 命令：发送给计算机的一条指令，一般是通过键盘或鼠标发送的。
- 命令行：shell 提示之后可以输入命令的地方。
- 图形桌面：图形用户接口（GUI）的可见部分。桌面就是用户主目录图标和计算机图标位置。您可以使用喜欢的背景、颜色和图片定制自己的桌面。
- 图形用户接口（GUI）：图形用户接口是对交互式窗口、图标、按钮和面板的一般术语。用户可以利用这些交互式窗口、图标、按钮和面板执行启动应用程序以及用鼠标或键盘打开文件等操作。
- 图标是一些小的图片。它们表示一个应用程序、文件夹、快捷方式或者是系统资源（例如磁盘驱动器）
- man 手册页和 info 手册页：man 手册页和 info 手册页为用户提供了对命令或文件的简要介绍。例如在 shell 提示符后输入 man su（或 info su），系统就会显式命令 su 的手册。输入 q 即可退出手册。
- 面板：它是一个桌面的工具条，位于桌面的底部（如图 2-1）。面板包含了应用程序按钮和用于启动一般用户程序的图标。



图 2-1 桌面面板

- 根（root）：根是在系统安装期间创建的系统管理员（即超级用户）帐户。他（她）拥有对任何系统资源的访问权限。如果您想执行修改管理员帐户密码或是运行配置工具就必须以根用户身份登陆系统。

- RPM：RPM 是 RPM 包的管理工具。它是一个软件包。您可以将它安装在自己的系统上。

- Shell 提示（prompt）：它是用户和操作系统之间的命令行接口（如图 2-2）。Shell 会解释用户输入的命令，将其传递给操作系统。

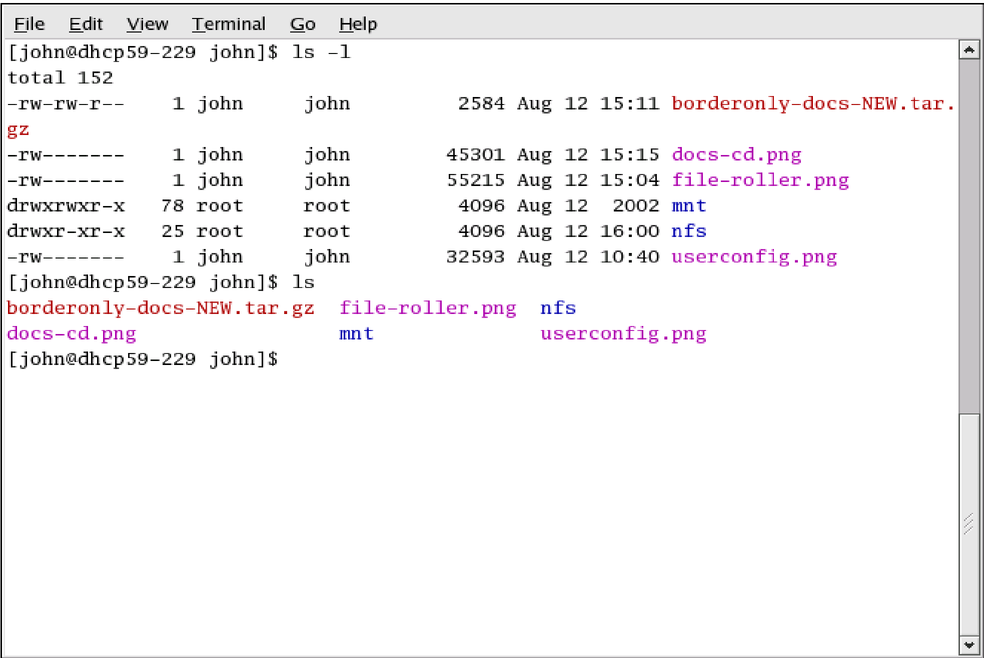


图 2-2 shell 提示

- su 和 su -：命令 su 是用于转换用户的。你可以使用该命令转换到根用户或者其他用户。使用命令 su –可以使您的根（root）位于根帐户的 shell 环境中。

- X 或 X 窗口系统：该术语指的是图形用户接口环境。如果您是“在 X 中”或者“运行 X”，那么您就是在图形用户接口（GUI）环境下工作，而不是控制台环境。

2.1.3 登录

下一步是登录您的 GTES10 系统。当你登录系统的时候，其实就是您正在向系统介绍您自己（也是系统向您授权）。如果您输入了错误的密码，系统将拒绝您登录。GTES10 用帐户来管理特权、保护系统安全。不是所有的帐户都是平等的，各个帐户对文件和服务的访问权限是不同的。

如果您已经创建了一个帐户，并且用该帐户登录了系统，那么您可以直接跳到“使用图形桌面”一节，如果您仅仅创建了根用户，那么请参考“创建帐户”一节。

如果您已经创建了一个普通用户帐户，那么我们强烈推荐您以普通用户身份登录您的系统，以免因为误操作而损坏系统。

2.1.3.1 以图形界面登录

当系统被引导启动之后，屏幕上将会出现如图 2-3 所示的图形登录界面。如果您没有在最初设置网络时设置您的计算机名，那么将会使用默认名 localhost。

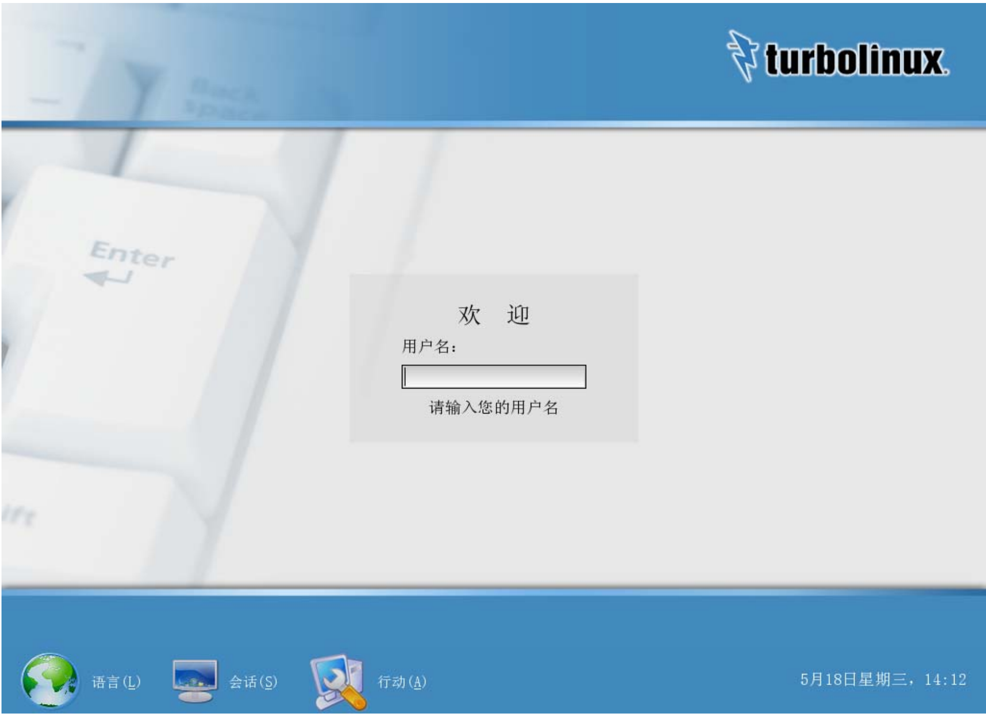


图 2-3 图形登录界面

如果以根用户身份登录系统，就在提示筐内输入 root，然后按回车键，系统会提输入根用户的秘密，输入系统安装时设定的根用户密码，然后按回车即可登录系统。如果想以普通用户登录系统，输入普通用户名，然后按回车，等系统提示输入密码后，在提示筐内输入用户密码，再按回车即可。

如果您是以图形界面登录系统的，那么系统将自动为您启动图形桌面。

2.1.3.2 虚拟控制台登录

在系统安装期间，如果您没有将安装方式选择成工作站或个人桌面，并且选择了文本方式登录，那么当您的系统引导启动后将会出现如下的文本登录界面。

```
GTES10 (Zuma)
```

```
Linux 2.6.9-5.8 on i686 (localhost.localdomain)

VC: tty1


localhost login:
```

如果您没有在最初设置网络时设置您的计算机名，那么将会使用默认名localhost.localdomain。

如果以根用户身份登录系统，就在提示符后输入 root，然后按回车键，系统会提输入根用户的秘密，输入系统安装时设定的根用户密码，然后按回车即可登录系统。如果想以普通用户登录系统，输入普通用户名，然后按回车，等系统提示输入密码后，在提示符后输入用户密码，再按回车即可。

登录系统之后，您可以执行命令 startx 来启动图形桌面。

2.1.4 图形界面

当您启动了 X 窗口系统之后，屏幕上就会出现如图 2-4 所示的图形界面(即桌面)。GTES10 以 KDE 做为默认的桌面，具体细节请参考“使用图形桌面” 一节。

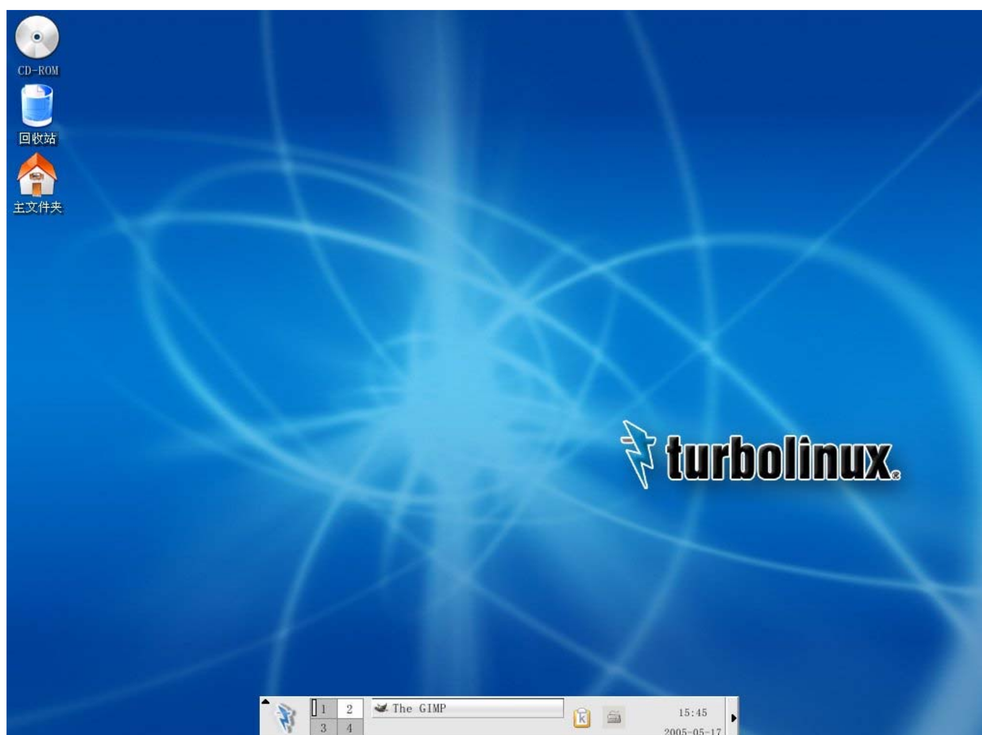


图 2-4 KDE 桌面

2.1.5 打开 shell 提示（prompt）

桌面对用户提供了访问 shell 提示的功能。Shell 提示是一个应用程序。它允许用户输入命令行的方式工作，而不依赖图形界面。打开 shell 提示的步骤为：点击主菜单，选择“应用程序->系统工具->终端”。您也可以用右键点击桌面的空白处，然后选择打开终端的方式来启动 shell 提示。关闭 shell 提示的方式有三种。第一种是点击 shell 提示右上角的 X 按钮；第二种是在 shell 提示中输入 exit，然后按回车；第三种是在 shell 提示中按[Ctrl]-[D]。如果您想对 shell 提示有进一步的了解，请参考“shell 提示基础” 一节。

2.1.6 创建用户帐户

当系统安装的过程中，会提示用户创建一个普通帐户。如果您在那时没有创建，那么最好在安装完毕后自己创建一个普通用户的帐户，而不是直接以根用户身份登录。

创建帐户的方法有两种：第一种是用图形用户管理器创建，第二种是在 shell 提示下用命令行创建。

2.1.6.1 用图形用户管理器创建用户

第 1 步：在主菜单中选择“系统设置->用户和组”。

第 2 步：如果您不是以根用户身份登录的，系统会提示您输入根用户帐户的密码。

第 3 步：出现如图 2-5 的用户管理器窗口。点击添加用户图标。

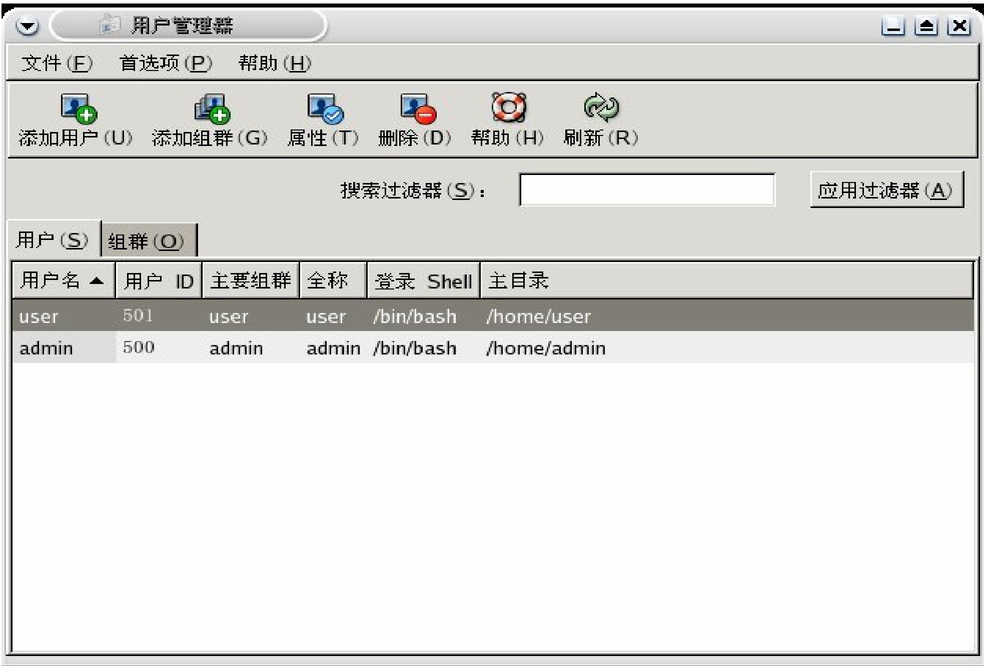


图 2-5 用户管理器

第 4 步：在创建新用户对话框中输入用户信息和密码。

第 5 步：点击确定后，新用户的信息就会出现在用户列表中了。

2.1.6.2 用 shell 提示下命令行方式创建用户

第 1 步：打开一个 shell 提示。

第 2 步：如果您不是以根用户身份登录的，则在 shell 提示中输入命令 su - 然后输入根用户的密码。

第 3 步：输入命令 useradd，在其后紧跟要创建的用户名，然后输入回车。

第 4 步：输入命令 passwd，在其后紧跟要创建的用户名，然后输入回车。

第 5 步：在出现的 New password:提示后输入用户密码。

第 6 步：在 Retype new password:提示后再次输入刚才的密码，创建新帐户的工作就算完成了。

2.1.7 文档和帮助

GTES10 为用户提供了多种文档以帮助用户配置和使用系统。系统所带的文档包括三种。第一种是手册页。它提供了重要应用程序和文件的详细的说明。第二种是信息页。信息页将应用程序的信息用上下文敏感的菜单进行分割。第三种是帮助文件。它位于图形应用程序的主菜单条中。

2.1.7.1 使用 man

用户可以通过在 shell 提示中输入命令 man 和可执行文件名来访问手册页。例如，想访问 ls 的手册页只要在 shell 提示中输入 man ls 屏幕上就会显示如图 2-6 所示的信息，输入[q]即可退出。

```
File  Edit  View  Terminal  Go  Help
LS(1)                          User Commands                          LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information  about  the FILEs (the current directory by default).
       Sort entries alphabetically if none of -cftuSUX nor --sort.

       Mandatory arguments to long options are  mandatory  for  short  options
       too.

       -a, --all
              do not hide entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
              print the author of each file
:
```

图 2-6 关于 ls 的 man 信息

2.1.7.2 man 自己的手册页

像其他的命令一样，man 也有自己的手册页，只要在 shell 提示中输入 man man 即可打开 man 的手册页。

2.1.8 注销

2.1.8.1 图形注销

如果您要注销您的桌面会话，可以选择桌面底部的“行动->注销”即可。当出现如图 2-7 所示的对话框后，选择注销即可。



图 2-7 注销确认

2.1.8.2 虚拟控制台注销

在虚拟控制台中只要输入 exit 或按[Ctrl]-[D]即可注销。

2.1.9 关闭计算机

2.1.9.1 图形关闭

在图 2-7 所示的对话框中选择关闭计算机，然后点击确认，即可关闭计算机。

2.1.9.2 虚拟控制台关闭

如果您是在虚拟控制台下工作，只要输入 halt 即可关闭计算机。

2.2 使用图形桌面

GTES10 以 KDE 做为默认的桌面。K 桌面环境（KDE）是一个图形化的桌面。它在功能上类似于 gnome 桌面。这一部分将会介绍 KDE 的基本应用：系统导航、文件和应用程序的使用、定制桌面。

如果您希望深入了解KDE，可以参考 http://www.kde.org/。

2.2.1 定制 KDE

KDE 是一个具有高度可配置性的桌面系统。打开控制中心，您可以看到控制中心列出了如下的配置选项。

2.2.1.1 KDE 组件

这一部分为用户提供了配置 Konqueror 文件管理器和定制某些文件操作的功能。您可以将文件关联到某个应用程序（例如可以将数据音乐文件关联到 xmms，而不是默认的播放器）。

2.2.1.2 外观和主题

这一部分为用户提供了对桌面环境可视部分的定制功能。您可以定制背景图并且配置字体、主题、图标、面板元素、屏幕保护，和窗口边界的外观。您也可以按照自己的喜好定制鼠标和键盘的事件，以提高您的工作效率。

2.2.1.3 区域和辅助功能

这一部分为用户提供了设置国家和语言的选项。

2.2.1.4 系统管理

这一部是高级的系统管理接口。其中的大部分选项都要求以根用户的身份才能配置。这一部分为用户提供了安装新字体、配置登录管理器、这种系统路径等很多功能。如果您对其中某一个选项做了修改，但又对该选项的功能不了解，那么我们强烈推荐您选择默认值按钮。

2.2.1.5 互联网和网络

这一部分为用户提供了网络和浏览器的配置功能。

2.2.2 Konqueror 简介

Konqueror 是 KDE 的文件管理器。它在功能上相当于 GNOME 的 Nautilus。Konqueror 提供了对系统和个人文件的图形显式。它允许您配置您的桌面和 GTES10 系统、访问网络资源等一些其他功能。Konqueror 会使用图标、面板和回收站。下面介绍 Konqueror 提供的一些功能。

2.2.2.1 用户主文件夹（home）

Konqueror 的默认行为是浏览器。它会在当前窗口中打开文件和目录，而不是在新打开的 Konqueror 中打开文件和目录。您可以像使用 Firefox 或其他浏览器一样用右键点击文件或目录，然后选择用新建标签打开，使得在新建的标签中打开文件或目录。

2.2.2.2 回收站

像其他操作系统一样，KDE 也有回收站。回收站中的文件直到选择清楚的时候才会被删除。只要您用鼠标双击桌面上的回收站图标就可以打开回收站。打开的回收站就如同一个 Konqueror 窗口。它允许您将文件移进移出。如果您用右键点击回收站，然后选择清空回收站，就可以将回收站清空。

2.2.2.3 可移动介质

KDE 可以对可移动介质进行操作。其中包括磁盘、CD-ROM 和 DVD-ROM。

2.2.2.3.1 磁盘

在访问磁盘之前必须先挂载磁盘，使用完毕后必须卸载磁盘。可以使用 Konqueror 挂载磁盘。首先打开 Konqueror 窗口，然后从工具条中选择“转到->设备”，双击软盘图标就可以将软盘挂载上来。当完成操作后，回到 Devices 目录，然后右键选中软盘图标，选择卸载，就可以卸载软盘。

2.2.2.3.2 CD-ROM 和 DVD-ROM

当您将 CD 或 DVD 插入驱动器后，系统会自动将其挂载。打开 Konqueror 浏览器，在工具条工具条中选择“转到->设备”，双击相应的图标就可以打开 CD 或 DVD 了。如果插入的 CD 或 DVD 没有被自动挂载，那么您只要打开 Konqueror 浏览器，在工具条工具条中选择“转到->设备”，然后用右键点击 CD 或 DVD 的图标，选择挂载，就可以挂载 CD 或 DVD。当您想弹出 CD 或 DVD 时，可以打开 Konqueror 浏览器，在工具条工具条中选择“转到->设备”，然后用右键点击 CD 或 DVD 的图标，选择弹出，就可以卸载并弹出 CD 或 DVD。

2.2.2.4 定制 Konqueror

Konqueror 的行为也可以被定制。打开 Konqueror，在工具条中选择“设置->配置 Konqueror”就可以打开 Konqueror 的配置窗口（如图 2-8 所示）。



图 2-8 Konqueror 配置窗口

在左边的窗格中是可定制选项的图标列表。点击其中的任意一个图标，就会在右边窗格内显示出相应的配置选项。例如，点击外观图标后就会在右边的窗格内显示出字体选择、Konqueror 窗口大小选择等配置项。修改配置项后，点击应用按钮可以保存配置，然后点击确定按钮就完成了配置工作并退出了配置窗口。

2.2.3 使用 Konqueror

Konqueror 是 KDE 桌面的文件管理器和 web 浏览器。Konqueror 允许用户配置自己的 KDE 桌面、配置 GTES10 系统、播放多媒体文件、浏览数字图片、到网上冲浪以及其他一些功能。这一部分主要介绍 Konqueror 的使

用。

您只要在桌面上点击图标，就可以启动 Konqueror。

Konqueror 可以使用用户浏览自己的主（home）目录以及整个 GTES10 系统，在浏览过系统之后，可以点击工具栏中的 Home 按钮直接回到主目录。

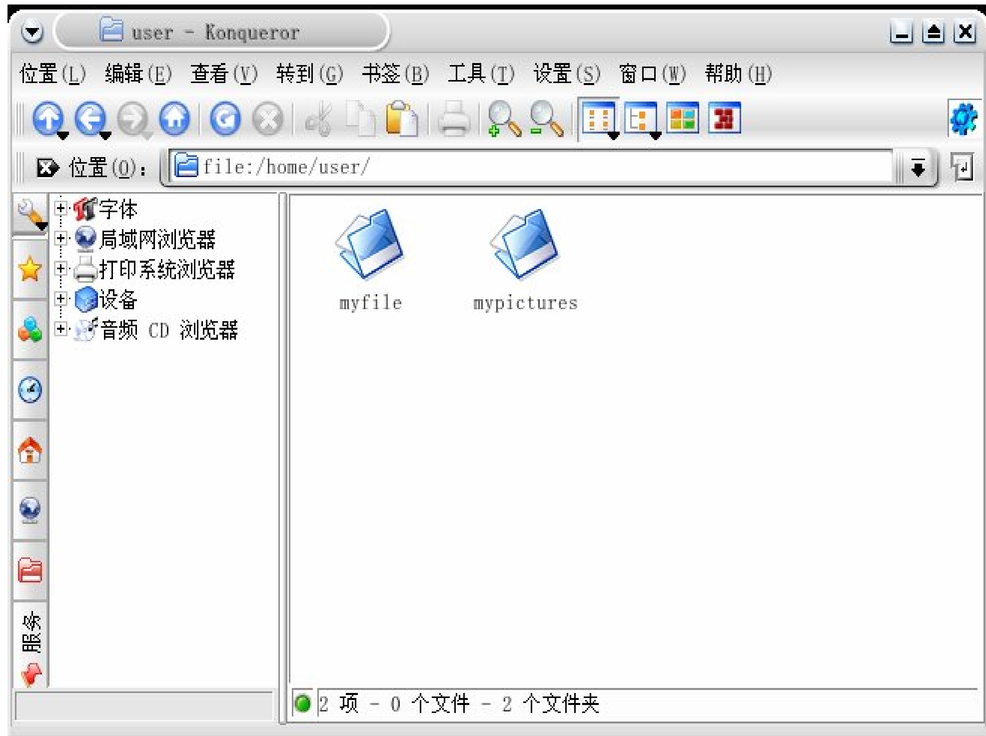


图 2-9 Konqueror 文件管理器

您可以点击右边窗格中的文件夹图标或者使用 Konqueror 导航面板中的分层文件系统浏览器浏览文件系统。主窗口筐中的文件或目录可以被移动或拷贝到另外的文件夹中，也可以被放入回收站中。您也可以用右键点击文件或文件夹，然后选择删除来删除文件或文件夹。

Konqueror 也可以显示小图标、图片、PostScript/PDF 文件和 web 文件。它还可以预览数字音频文件。

2.2.3.1 导航面板

Konqueror 另外一个很有用的特性就是导航面板。默认情况下导航面板位于 Konqueror 窗口的左边。用户可以利用导航面板上的图标按钮便利地访问各种系统资源。图 2-10 展示的就是导航面板。



图 2-10 Konqueror 导航面板

2.2.4 使用 KDE 桌面

如前面所述，KDE 图形桌面具有各种应用窗口、启动图标、面板和其他工具。在下面的章节中我们将详细介绍这些工具。

2.2.4.1 在桌面上增加应用程序启动图标

一些用户喜欢在桌面上直接访问经常使用的应用程序，而不愿意到菜单中去找。为了实现这一个目的，用户可以在桌面上创建用户可以在桌面上创建应用程序启动图标。一般有三种可行的方法：

- 将应用程序启动图标从主菜单中拖出来，然后放到桌面上。
- 将应用程序启动图标从面板中拖出来，然后放到桌面上。
- 在桌面上手工创建应用程序启动图标。

一般情况下，只要从面板或菜单中将应用程序启动图标拖到桌面上即可。但如果菜单和面板都没有应用程序启动图标，就需要自己创建了。

手工创建应用程序启动图标的步骤如下：

第 1 步：您应该知道要创建启动图标的应用程序的名称。

第 2 步：您应该知道应用程序文件的位置。您可以用 which 命令来寻找应用程序文件的位置。

第 3 步：用鼠标右键点击桌面上的空白部分，选择“新建->文件->应用程序链接”。

第 4 步：当出现对话框（如图 2-11 所示）后，输入如下内容

描述：启动图标的名字。

注释：对该应用程序的简单描述，该项是可选的，可以不填。

命令：应用程序可执行文件的路径。

工作路径：应用程序的工作路径。

第 5 步：填写完毕后，点击确定按钮。



图 2-11 创建应用程序启动图标窗口

2.2.4.2 配置桌面

右键点击桌面上的空白部分，选择配置桌面，即可出现配置桌面窗口。桌面配置窗口包含以下图标：背景、行为、多个桌面、屏幕保护程序、显示。您可以点击任意一个图标来选择配置的选项。


配置 - 桌面
背景
行为
多个桌面
屏幕保护程序
显示
更改背景设置
桌面设置(D)：
全部桌面
背景
没有图片(N)
图片(P)：
/usr/share/backgrounds/images/default.png
放映幻灯片(S)：
设置(U)...
选项
位置(T)：
缩放
颜色(L)：
垂直渐变
混和(B)：
不混和
平衡：
反转
高级选项...
帮助(H)
默认值(D)
确定(O)
应用(A)
取消(C)

图 2-12 桌面背景配置



图 2-13 虚拟桌面配置

如果要配置多个桌面，只要点击多个桌面图标，选择图标数量，在文本区输入各个桌面的名称，然后点击应用按钮，再点击确定按钮即可。

2.2.5 使用面板

面板位于桌面底部。默认情况下，面板包含主菜单和其他一些如 web 浏览器、邮件客户端、编辑器之类的常用应用程序图标。

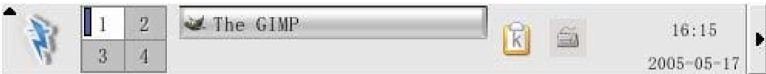


图 2-14 面板

applets 是运行在面板上的小应用程序。面板上的 applets 可以分为这几类：

用于系统监控的 applets、用于显示时间和日期的 applets、启动应用程序的 applets。有一部分 applets 是默认在面板上运行的。这一小节将详细介绍面板上的 applets。

2.2.5.1 桌面切换器

默认情况下，KDE 提供了四个桌面。这四个桌面都是独立的。用户可以利用桌面切换器在多个桌面之间进行切换。这样可以使用户的程序不必挤在一个桌面上。图 2-15 显示的就是四个桌面的桌面切换器。



图 2-15 桌面切换器

例如，当您在一个桌面上用 Evolution 写信息的时候，您还可以在另外一个桌面用 Mozilla 浏览 web。

2.2.5.2 任务条

如图 2-16 所示，任务条上显示了在所有窗口运行的应用程序。您可以点击相应的图标以最大化或最小化应用程序窗口。任务条也是可配置的。你可以用右键点击任务条左边的箭头，选择配置任务条即可。



图 2-16 任务条

2.2.5.3 主按钮

主按钮是 KDE 的中心点。点击主按钮就会出现一张大的主菜单。您可以在主菜单中选择执行各种任务，例如启动应用程序、查找文件、配置桌面等。主菜单中还包含了一些子菜单。它们将应用程序分成了若干个类，

其中包括图像、互联网、办公、游戏等等。

您可以从主菜单中选择锁住会话。这样屏幕就会显示为一个密码保护的屏幕保护窗口。您也可以通过在命令行中运行应用程序来注销您的 KDE 会话。

2.2.5.4 配置面板

像 KDE 中其他的工具一样，面板也是可以配置的，只要用右键点击面板中空白的部分，然后选择配置面板就会出现如图 2-17 所示的面板配置窗口。



图 2-17 面板配置窗口

2.2.5.5 添加 applets 到面板中

右键点击面板的空白部分，选择“添加->应用程序按钮”，然后选择您想要添加的应用程序即可。

2.2.6 用 Konqueror 浏览 web

Konqueror 不仅仅是一个文件浏览器（如图 2-18），也是一个 web 浏览器。点击主菜单，选择“因特网->Konqueror”就可以启动 Konqueror。将要访问的 URL 输入到位置后的空白处中然后按回车，就可以访问相应的网页了。点击工具条上的刷新按钮或按功能键 F5 就可以刷新网页。点击工具条上的停止按钮或按 Esc 键可以停止载入当前网页。点击工具条中的后退可以访问前一个访问过的网页，点击前进可以访问后一个访问过的网页。

Konqueror 允许用户在同一个浏览器窗口中的不同标签内不同载入多个网页。点击工具条中的位置，选择新建标签，就可以在同一个浏览器窗口中打开一个新的标签，然后输入 URL，就可以在新标签中打开网页了。

如果用户想了解更多的信息，可以通过帮助阅读 Konqueror 的手册（如图 2-19）。

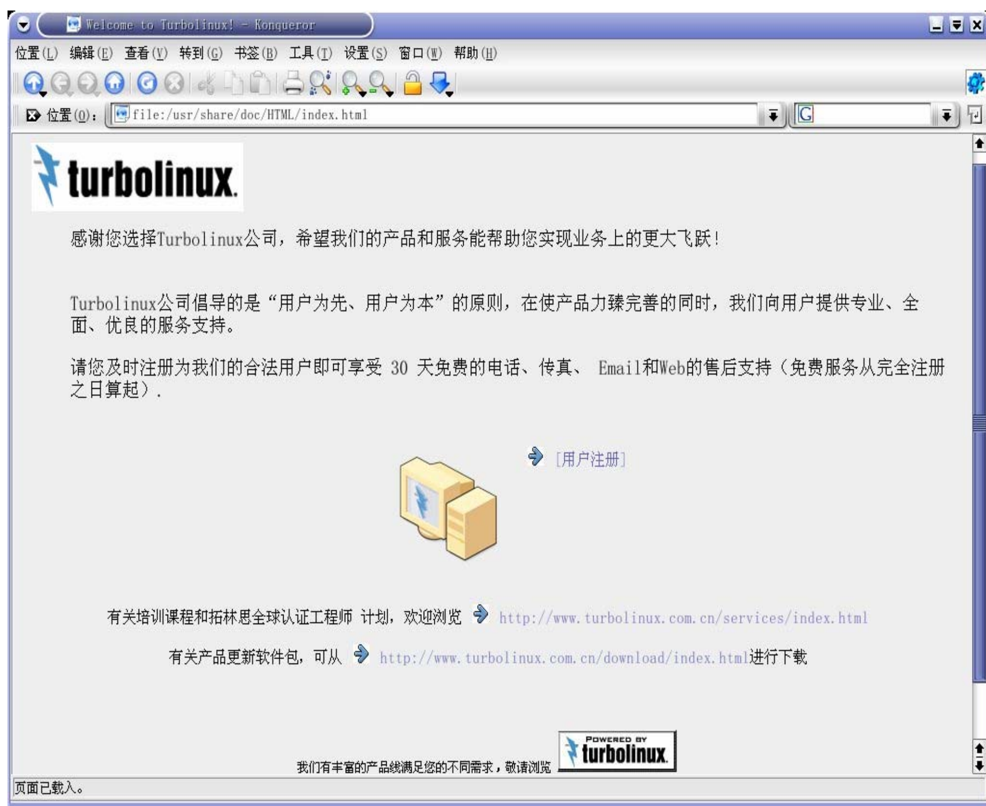


图 2-18 Konqueror 欢迎界面

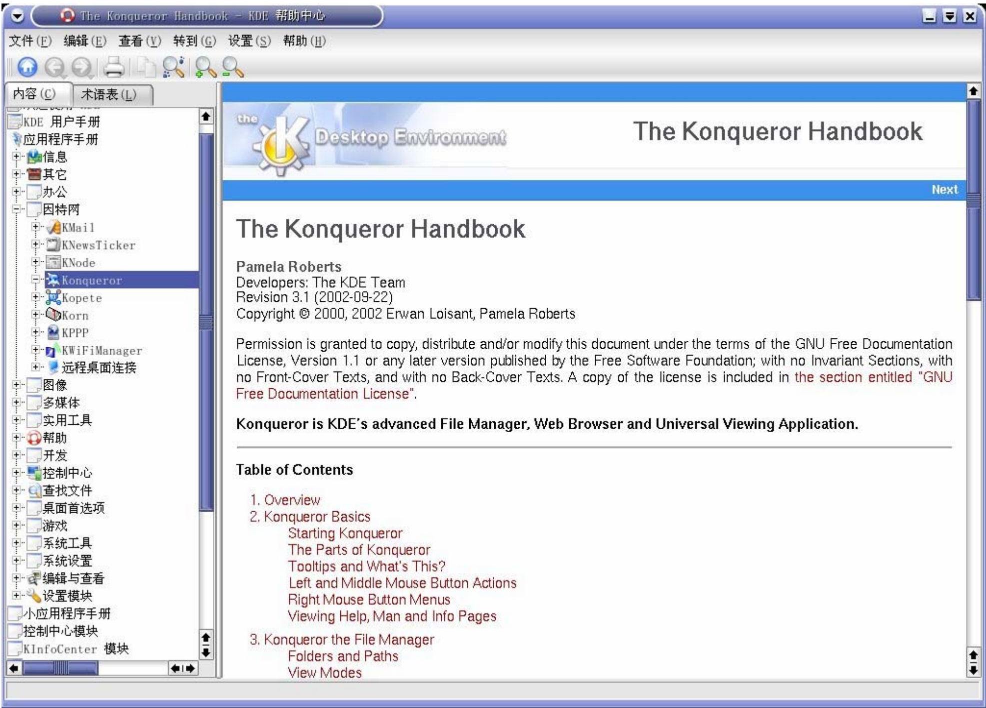


图 2-19 Konqueror 手册

2.2.7 用 Konqueror 查看图片

您也可以像使用 Nautilus 一样使用 Konqueror 文件管理器查看图片。Konqueror 会自动在窗口中创建小的预览图标。当您双击小图标后，Konqueror 会在窗口中按图片原始大小显示图片（如图 2-20）。

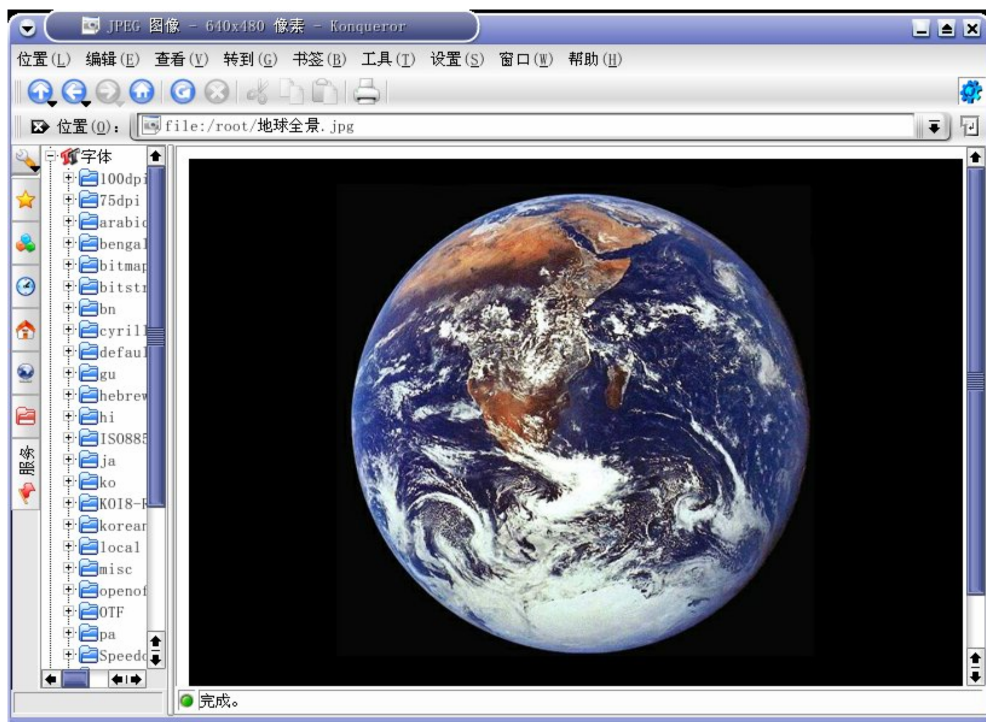


图 2-20 在 Konqueror 中查看图片

如果想放大或缩小图片，您首先必须修改 Konqueror 显示图片的方式。您可以从窗口的菜单中选择“视图->视图模式->kview 图像查看器”，Konqueror 就会重新显示图片，然后您就可以用图 2-21 中显示的工具条对图片进行旋转、放缩。



图 2-21 图片视图配置工具条

2.2.8 KMail

KMail 是 KDE 的电子邮件工具。它具有类似于 Evolution 的图形化的界面。

您可以用 KMail 收发邮件。您可以点击主菜单，选择“因特网->Kmail”来打开 KMail。

在使用 KMail 之前，您必须先配置 KMail。从 KMail 的工具条中选择“设置->配置 Kmail”，就可以打开 KMail 的配置工具。

KMail客户端的配置窗口包含如下部分：身份、网络、外观、编写器、安全和杂项。如果想要发送和接收邮件，您必须先对身份和网络这两个部分进行设置。如果想获取更多关于KMail的信息，您可以参考KMail的手册或访问KMail的主页 http://kmail.kde.org。

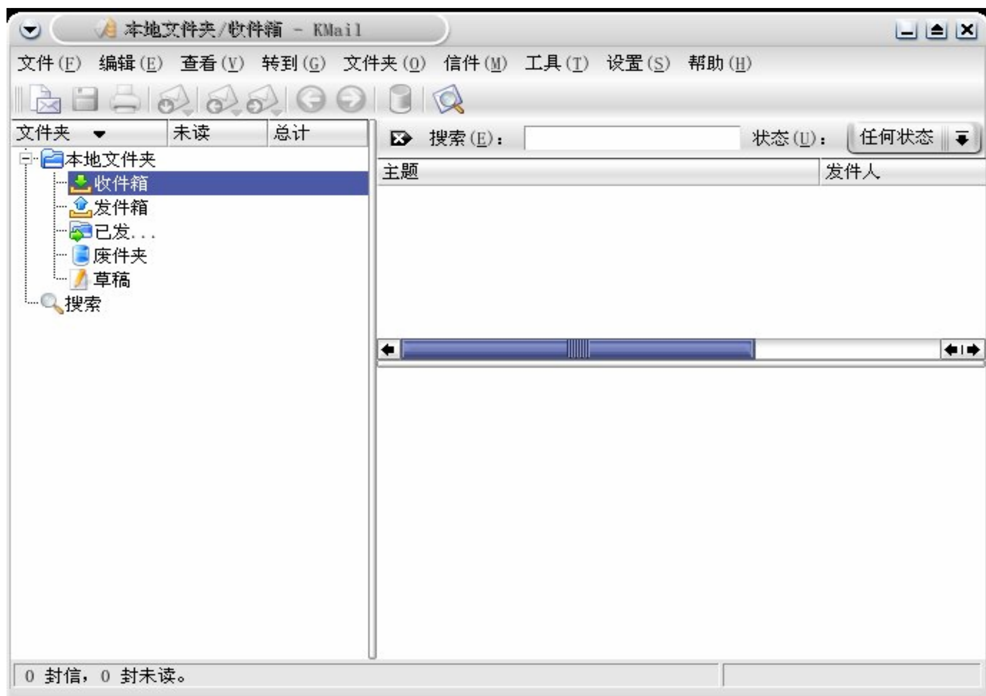


图 2-22 KMail 主窗口

一旦设置完毕，您就可以点击 KMail 左上角的检查邮件图标来收取和发送邮件了。左边的文件夹允许用户查看已经接收的邮件、已经发送的邮件、将要发送的邮件、已经发送的邮件等。如果想要编写新邮件，您可以工具

条上的新信件图标 就会打开如图 2-23 的新邮件编写窗口。

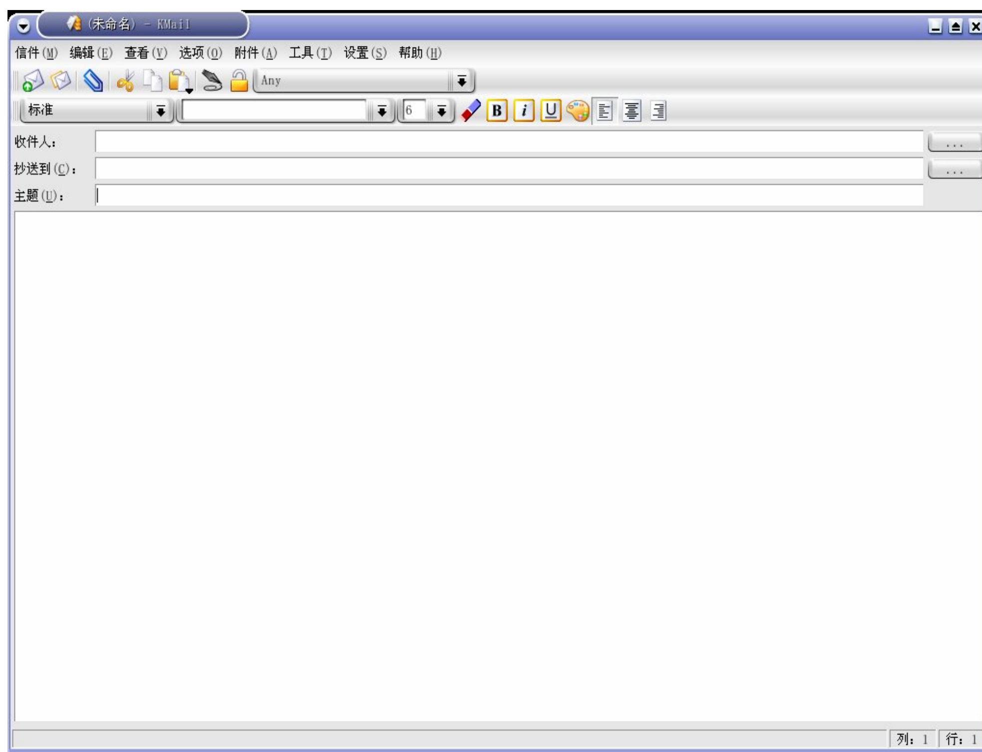


图 2-23 KMail 的新信件窗口

一旦编写完信件，你只要填写好对方邮件地址，然后点击工具条上的发送图标 就可以将邮件发送出去。

2.2.9 注销 KDE

有两种方法可以注销 KDE。第一种是从主菜单中选择注销，然后点击注销按钮。另外一种方法是右键点击桌面的空白处，选择注销“用户”。



图 2-24 KDE 注销窗口

2.2.10 帮助

您可以通过系统的帮助手册更全面地了解 KDE。打开帮助的步骤是：点击主菜单按钮，选择帮助，以打开系统的帮助（如图 2-25 所示）。

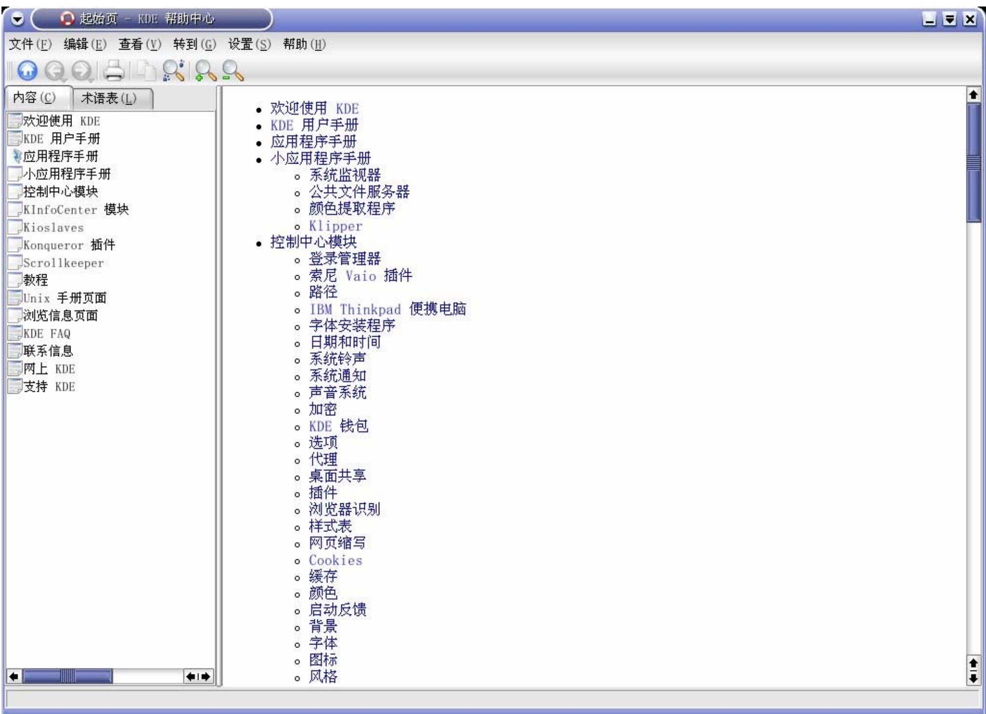


图 2-25 帮助

2.3 管理文件和目录

这一部分主要介绍 GTES10 的文件系统。至于如何用 shell 提示管理文件和目录，请参考“shell 提示基础” 一节。

2.3.1 文件系统术语

在介绍文件系统之前，我们先介绍一些术语。

- 扩展名

扩展名指的是文件名后部更在符号“.”之后的部分。例如，在文件名 foo.text 中 text 就是扩展名。

- 路径

路径指的是目录和子目录组成的字符串。您可以根据它到底文件系统中指定的位置。

- 根用户访问权限

拥有根用户访问权限指的是必须用根用户的帐户登录到系统。这意味着如果您如果拥有根用户访问权限，就可以对系统进行任何操作，所以必须小心使用根用户权限。

- 根目录

根目录指的是文件系统最顶层的目录。不要将根目录“/”和根用户的主目录“/root”混淆了。

2.3.2 一张更大的文件系统视图

任何一个操作系统都有自己的对数据的存储方法。在 GTES10 中，文件是被存放在目录中的。目录还可以包含子目录。子目录还可以包含子目录和文件。

在 GTES10 的文件系统中，一共有两种路径。一种是相对路径，指的是从当前目录开始到文件系统中某一位置的路由。另外一种是绝对路径，指的是从根目录开始到文件系统中某一位置的路由。例如，当前路径是/root，那边到达/tmp 的相对路径为../tmp，而绝对路径为/tmp。

2.3.3 管理文件

如果对 linux 来说您是一个新手，那么您可能会觉得 linux 文件系统中的文件名看起来有点古怪。您可能觉得 Linux 中文件名的扩展名好多以前都没见过。Linux 中有有的文件名有多个扩展名，有些则没有扩展名。

2.3.3.1 文件类型

2.3.3.1.1 压缩和归档文件

- .bz2－用 bzip2 压缩的文件
- .gz－用 gzip 压缩的文件
- .tar－用 tar 归档的文件
- .tbz 或.tar.bz－用 tar 归档后，再用 bzip 压缩的文件
- .tgz 或.tar.gz－用 tar 归档后，再用 gzip 压缩的文件
- .zip－用 gzip 压缩的文件

2.3.3.1.2 文件格式

.au－音频文件

- .gif－GIF 图像文件（Graphics Interchange Format 的缩写）
- .html 或.htm－HTML 文件（Hyper Text Markup Language 的缩写）
- .jpg－JPG 文件（Joint Photographic Experts Group 的缩写）

- .pdf－文档电子图像文件，PDF 表示 Portable Document Format
- .png－PNG 图像文件（Portable Network Graphic 的缩写）
- .ps－PostScript 文件，这是一种用于打印的格式
- .txt－简单的 ASCII 文本文件
- .wav－音频文件
- .xpm－图像文件（X Pixelmap 的缩写）

2.3.3.1.3 系统文件

- .conf－配置文件，也可以用扩展名.cfg 表示
- .lock－加锁文件，表示一个程序或设备是否正在被使用
- .rpm－用于安装软件的 Red Hat 包管理（Red Hat Package Manager 的缩写）文件

2.3.3.1.4 程序和脚本文件

- .c－C 语言源代码文件
- .cpp－C＋＋源代码文件
- .h－C 或 C＋＋头文件
- .o－程序目标文件
- .p－perl 脚本文件
- .py－python 脚本文件
- .so－库文件
- .sh－shell 脚本文件
- .tcl－TCL 脚本文件

2.3.3.1.5 命名习惯

- 点文件

在 linux 中文件名以符号“.”开始的文件称为点文件。这种文件是隐藏文件。在图像工具下可以选择“视图->显示隐藏文件”来查看，也可以在 shell 提示下用 ls –a 来查看。

- 在文件名中使用符号

您可以在文件名中使用标点符号，但要明确的是各种标点符号都有自己特殊的含义。如果使用不当，则容易出错。所以我们建议您一般情况下不要在文件名中使用标点符号。有一些特殊的符号是不能出现在文件名中的，例如“/”、“.”、“..”。

- 在文件名中使用多个扩展名

多扩展名文件中的扩展名都是以“.”分隔的。处理多扩展名文件一般要使用多个程序或命令。多扩展名文件一般都是归档压缩文件。

2.3.3.2 查看文件类型

对于一些没有扩展名的文件，我们如果不能从文件名看出文件的类型，那么可以借助命令 file。例如有一个文件名为 saturday 的文件，如果要查看它的文件类型，我们只要在 shell 提示中输入 file saturday 即可显示文件的类型。

2.3.4 文件压缩和归档

2.3.4.1 用 file roller

2.3.4.2 在 shell 提示下压缩文件

2.3.4.2.1 bzip2 和 bunzip2

如果要用 bzip2 压缩一个文件，只要在 shell 提示下输入如下命令：

```
bzip2 filename
```

就另外会生成一个压缩文件 filename.bz2。

如果想解压缩这个文件，只要在 shell 提示下输入如下命令：

```
bzunip2 filename.bz2
```

就会生成一个解压缩的文件 filename，而原来的压缩文件 filename.bz2 则会被删除。

bzip2 可以一次压缩多个文件和目录。具体操作是在 shell 提示下输入如下命令：

```
bzip2 filename.bz2 file1 file2 file3 /usr/work/school
```

注意两个文件或目录之间必须以空格分隔。

2.3.4.2.2 gzip 和 gunzip

如果要用 gzip 压缩一个文件，只要在 shell 提示下输入如下命令：

```
gzip filename
```

就另外会生成一个压缩文件 filename.gz。

如果想解压缩这个文件，只要在 shell 提示下输入如下命令：

```
gunzip filename.gz
```

就会生成一个解压缩的文件 filename，而原来的压缩文件 filename.gz 则会被删除。

gzip 可以一次压缩多个文件和目录。具体操作是在 shell 提示下输入如下命令：

```
gzip –r filename.bz2 file1 file2 file3 /usr/work/school
```

注意两个文件或目录之间必须以空格分隔。

2.3.4.2.3 zip 和 unzip

如果要用 zip 压缩一个文件，只要在 shell 提示下输入如下命令：

```
zip –r filename.zip filesdir
```

就另外会生成一个压缩文件 filename.zip。其中 filesdir 表示要压缩的目录，-r 表示对目录 filesdir 下的所有文件和子目录做递归处理，即将 filesdir 下的所有文件和子目录都放到压缩文件中。

如果想解压缩这个文件，只要在 shell 提示下输入如下命令：

```
unzip filename.zip
```

就会生成一个解压缩的文件 filename，而原来的压缩文件 filename.gz 则会被删除。

zip 可以一次压缩多个文件和目录。具体操作是在 shell 提示下输入如下命令：

```
zip –r filename.bz2 file1 file2 file3 /usr/work/school
```

注意两个文件或目录之间必须以空格分隔。

2.3.4.3 在 shell 提示下对文件归档

使用 tar 是对文件进行备份和归档的一种好办法。下面介绍一些 tar 的选项：

- -c－创建新的归档文件
- -f－当使用-c 选项时，指明要创建的归档文件名；当使用-x 时，指明要解开的文件名
- -t－显示归档文件中的文件列表
- -v－显示归档文件被解包时的进展
- -x－解开归档文件
- -z－用 gzip 压缩归档文件
- -j－用 bzip2 压缩归档文件

如果要创建归档文件，只需输入：

tar -cvf filename.tar directory/file

在这个例子中，filename.tar 表示要创建的归档文件名，directory/file 表示要放入归档文件中的目录和文件。

您可以用文件和目录列表的形式同时归档多个文件和目录。例如：

```
tar -cvf filename.tar /home/mine/work /home/mine/school
```

列表中的元素必须用空格分隔。

要列出归档文件中的内容，可以输入：

```
tar -tvf filename.tar
```

要解开一个归档文件，可以输入：

```
tar -xvf filename.tar
```

默认情况下 tar 命令并不会对被归档的文件进行压缩。如果要对归档文件用 bzip 压缩，可以使用选项-j：

```
tar -cjvf filename.tbz file
```

解开上面这个压缩归档文件，可以输入：

```
tar -xjvf filename.tbz
```

如果要对归档文件用 gzip 压缩，可以使用选项-z：

```
tar -czvf filename.tgz file
```

解开上面这个压缩归档文件，可以输入：

```
tar -xzvf filename.tgz
```

2.3.5 管理目录

在大多数情况下，我们对目录和文件是一样处理的。用户可以对它们进行创建、拷贝、删除等操作。

2.3.5.1 创建目录

用户只有在自己具有写权限的目录下才能创建子目录。每个用户对自己的

主目录和/tmp 目录都有写权限。创建目录的命令为：

```
mkdir <directory-name>
```

2.3.5.2 删除目录

删除一个空目录的命令为：

```
rmdir <directory-name>
```

如果要删除一个非空目录，则需要用命令 rmdir –rf <directory-name>。

2.3.5.3 点目录

应用程序创建的点目录就和点文件一样。点文件是隐藏的文件，而点目录是隐藏的目录。点目录下一般存放的是配置文件和应用程序所需的其他文件。

2.4 shell 提示基础

2.4.1 为什么使用 shell 提示

图形环境对用户来说确实是非常方便，但许多操作在 shell 环境下会更快捷。Shell 提示看上去和用户所熟悉的其他命令行接口非常相似。用户在 shell 提示中输入命令，shell 解释用户输入的命令，然后通知操作系统执行这些命令。

这一节我们将介绍如何访问文件系统，如何对文件进行操作，以及如何执行一些简单的管理任务，和其他一些 shell 的基础知识。



图 2-26 shell 提示

2.4.2 shell 基础

2.4.2.1 shell 提示术语

- 命令行

命令行是命令的选项所在的部分。下面是一个命令行的例子：

```
command –options <filename>
```

- shell 提示

shell 提示是屏幕上的一个标记，在这个标记后可以输入命令行。下面是一个 shell 提示的例子：

```
[username@localhost.localdomain username]$
```

- shell

shell 是一个接收用户命令，对其进行解释，然后传递给操作系统执行的程序。

- 终端窗口

终端窗口中包含了 shell 提示、命令行，以及 shell 的输出。

2.4.2.2 打开并使用 shell 提示

打开 shell 提示的方法有两种。一种是在主菜单或面板中选择；另一种是在桌面上用右键点击空白处，选择打开终端。点击 shell 提示窗口右上角的[X]图标或在命令行中输入 exit，再按回车就可以退出 shell 提示。终端窗口中的 shell 提示如下所示：

```
[username@localhost.localdomain username]$
```

普通用户的提示符为“$”，而根用户的提示符则为“#”。

2.4.2.3 shell 提示命令的结构

通常情况下运行在 shell 提示下的命令具有如下格式：

```
command -options <filename>
```

-options 和<filename>都是可选的：命令后可以不带选项或文件，或者带有多个选项和文件。当命令后带有多个选项时，应该将它们按组排列。例如，用长信息方式列出当前目录下所有文件和目录的操作：

```
ls –la
```

查询单个命令信息的方法有很多种，如果您想了解命令的具体使用方法，只要执行一下操作即可：

- 在 shell 提示后直接输入命令，然后按回车。例如，输入 cp 命令，shell 就会输出 cp 命令的简单帮助信息。但像 cat 这样的命令即使没有参数也能运行。如果您想要终止这个命令，可以按[Ctrl]-[D]。如果不管用，就按[Ctrl]-[C]。

- 在 shell 提示中输入

```
man command
```

shell 就会显示出关于 command 的手册页。按空格键可以向下翻页，按[B]可以向上翻页，按[Q]就可以退出手册页。

- 在 shell 提示中输入

```
info command
```

shell 就会显示出关于 command 的信息页。关于 info 命令的使用，可以用 info info 命令来查询。

2.4.3 用 pwd 确定您当前的目录

当用户在浏览目录时，经常会忘记当前所在目录的路径。这时您就可以在 shell 提示中输入 pwd 命令来查看当前目录的绝对路径（如图 2-27 所示）。



图 2-27 用 pwd 命令在 shell 提示中显示当前路径

2.4.4 在当前目录下对文件进行操作

2.4.4.1 用 ls 列出目录下的内容

使用命令 ls 可列出文件和目录，并了解到有关文件和目录的其他信息。它的格式如下：

```
$ ls [options] [file name] [directory name]
```

常用的选项有：

-l	不仅列出文件名，还应列出各文件的的全部细节信息。
-a	列出所有的文件，包括正常情况下隐含的文件。
-F	在文件名上附着一个符号，以显示文件的类型（可执行文件用星号“*”表示，目录用斜杠“/表示”），在 Turbolinux 中，ls 被设置为了 ls -F 的别名。

表 2-1 ls 常用的选项

如果未指定文件或目录名，那么将列出当前目录下的文件和子目录。

在下面给出的示例中，介绍了带有各种选项的 ls 命令。对于这里给出的示例，ls 命令是在目录/home/jon 下运行的。

在 Turbolinux 中，下述命令等同于-F 选项：

```
$ ls /home/jon
nsmail/          foo1       foo2
```

在 Turbolinux 中，命令 ls 的作用与 ls–F 相同。仅显示文件和目录：

```
$ ls -l /home/jon
total 352
```

```
drwx------ 2 jon        jon 1024 Aug 27 01:01 nsmail/
-rw------- 1 jon              jon 356352 Aug 27 07:25 foo
```

显示每个文件和目录的详细信息：

```
$ls –a /home/jon
./                  .bashrc             .lang/     .vimrc
../                 .elvisrc            .less          .xemacs/
.ICEauthority       .exrc               .mc/           .xsession*
.Xdefaults     .gnome/             .rhosts        nsmail/
.bash_history       .gnome-desktop/ .sawfish/      foo
.bash_logout        .gnome_private/ .screenrc      foo1
.bash_profile       .inputrc            .tcshrc        foo2
```

显示当前目录下的所有文件和目录，包括隐含文件、目录、以及子目录。

2.4.4.2 用 cp 拷贝文件或目录

使用命令 cp，不仅能将文件从一个位置拷贝到另一个位置，而且还能将整个目录及其子目录拷贝到不同的位置。命令 cp 的使用格式如下：

```
$ cp [options] [source filename | source directory name] [destination filename | destination directory name]
```

命令 cp 的常用选项如下：

-b	如果目标文件已存在，在执行拷贝操作前，会对已存在的文件进行备份。
-f	如果目标文件已存在，该文件将被强行覆盖。

-i	如果目标文件已存在，系统会询问你是否要覆盖该文件。如果回答“y”(是)，已存在的文件将被覆盖。如果给出的回答是“y”以外的，不会执行拷贝操作（在 TurbiLinux 中，cp 的别名被设为 cp-i)。
-u	如果目标文件已存在，只有当目标文件的日期比源文件的日期更早时，才会执行拷贝操作（如果目标文件的日期较新，拷贝操作不会进行)。
-p	在执行拷贝的过程中，保留源文件的属性（日期，所有者属性、许可权限)。
-v	显示拷贝操作的结果（源文件名->目标文件名)。
-R	以递归方式拷贝目录
-b	如果目标文件已存在，在执行拷贝操作前，会对已存在的文件进行备份。

表 2-2 cp 常用的选项

在下面的示例中，给出了 cp 命令与各种选项的使用方法，同时也包括系统响应：

```
$ cp -v file1.txt file2.txt

file1.txt -> file2.txt
```

使用-v 选项，会显示拷贝操作的结果。

```
$ cp -v file1.txt ../public

cp: overwrite '../public/file1.txt'? y

file1.txt -> ../public/file1.txt
```

在这个例子中，由于 Turbolinux 命令 cp 的别名是 cp –i，而且存在具有相同文件名的目标文件，系统会询问你是否允许覆盖目标文件，如果你给出肯定的回答，拷贝将继续进行，并会显示拷贝的结果。

```
$ cp -rv directory1/ directory2/
directory1/ -> directory2/
```

整个目录“directory1”被拷贝到了目录“directory2”。

2.4.4.3 用 mv 移动文件

使用命令 mv，可以将文件和目录从一个位置移动到另一个位置。它的使用格式是：

```
$ mv [options] [source filename | source directory name] [destination filename | destination directory name]
```

下面给出了常用的选项：

选项	说明
-b	如果目标文件已存在，在执行移动操作前，会对已存在的文件进行备份。
-f	如果目标文件已存在，该文件将被强行覆盖。
-i	如果目标文件已存在，系统会询问你是否要覆盖该文件。如果回答“y”(是)，已存在的文件将被覆盖。如果给出的回答是“y”以外的，不会执行移动操作（在 TurbiLinux 中，mv 的别名被设为 mv-i）。
-u	如果目标文件已存在，只有当目标文件的日期比源文件的日期更早时，才会执行移动操作（如果目标文件的日期较新，移动操作不会进行）。
-v	显示移动操作的结果（源文件名->目标文件名）。

表 2-3 mv 常用的选项

例如，如果打算将文件 file1.txt 移动到目录../public 下，可以采用下述方式使用命令 mv：

```
$ mv -v file1.txt ../public
```

```
mv: overwrite ’../public/file1.txt’? y
file1.txt -> ../public/file1.txt
```

在这个例子中，由于 Turbolinux 命令 mv 的别名是 mv –i，而且存在具有相同文件名的目标文件，系统会询问你是否允许覆盖目标文件，如果你给出肯定的回答，移动将继续进行，并会显示移动的结果。

2.4.4.4 用 mv 更改文件名

使用命令 mv，你还能更改文件的名称，它的格式是：

```
$ mv [options] [source filename | source directory name] [destination filename | destination directory name]
```

常见的选项有：

-v	显示移动操作的结果（源文件名->目标文件名）。

表 2-4 mv 更改文件名常用的选项

例如，要想将文件名 file1.txt 更改为 file2.txt，可以按下述方式使用命令 mv：

```
$ mv -v file1.txt file2.txt
file1.txt -> file2.txt
```

如果你省略了-v 选项，将不会出现要求进行确认的系统响应。要想了解更多的信息，请参阅 mv 的 的 手册页。

2.4.4.5 删除文件和目录

可以使用命令 rm 来删除文件和目录。也可以使用命令 rmdir 来删除空目录。这两个命令的格式是：

```
$ rm [options] [name of file to delete | name of directory to delete]
$ rmdir directoryname
```

下面给出了常用的选项：

-f	强行删除用户不具有写权限的一个文件或多个文件。
-i	如果目标文件已存在，系统会询问你是否要覆盖该文件。如果回答“y”（是），已存在的文件将被覆盖。如果给出的回答是“y”以外的，不会执行移动操作（在 TurbiLinux 中，rm 的别名被设为 rm-i）。
-v	显示删除操作的结果。
-r	以递归方式删除所有的文件、子目录和目录。

表 2-5 rm 常用的选项

例如：

要想删除位于当前目录下的文件 file1.txt，可以按下述方式运行命令 rm：

```
$ rm -v file1.txt
rm: remove ’file1.txt’? y
```

在这个示例中，由于 Turbolinux 命令 rm 的别名被设为了 rm-i，而且你也对系统的询问作了肯定的回答“y”，因此该文件将被删除。

如果你打算删除目录“/home/directory1”以及它的子目录，可以按下述方式使用 rm 命令：

```
$ rm -riv /home/directory1/
rm: descend into directory ’/home/directory1’? y
removing all entries of directory /home/directory1
rm: remove ’/home/directory1/file1.txt’? y
removing /home/directory1/file1.txt
rm: remove directory ’/home/directory1’? y
removing the directory itself: /home/directory1
```

如果打算删除空目录“directory2”，可以按下述方式执行命令 rmdir：

```
$ rmdir directory2
```

在本例中，系统不会给出要求进行确认的提示。要想了解更多的信息，请参见 rmdir 的手册页。

2.4.5 离开当前目录

要想从当前目录切换到不同的目录，可使用 cd 命令。它的格式是：

```
# cd [name of the desired directory]
```

如果你在使用 cd 命令时未带参数，即省略了目录名，那么命令 cd 会将你带到用户的主目录下。

没有必要总是为所需的目录指定完整的路径。可以使用下述参数：

. 当前目录

.. 当前目录的上一级目录

~ 用户的主目录

- 当前目录的前一个目录

举例说明，如果打算将当前目录（/home.jon）切换为目录/home，可使用下面给出的两个命令之一：

```
$ cd /home

$ cd ..
```

再举一例，如果打算将当前目录（/home）切换到用户的主目录，可使用下面给出的命令中的任何一种：

```
$ cd /home/jon

$ cd ./jon

$ cd jon

$ cd ~

$ cd
```

2.4.6 定位文件和目录

2.4.6.1 find

find 命令是一个目录树查找和执行的命令。它能根据要求在目录和所有子目录中查找文件，并且可以对匹配的文件运行任何命令或者 shell 脚本。

find 的使用语法如下：

```
find directories… options… action
```

参数选项以单词形式使用，例如：

-name name　　　　查找名为 name 的文件

-user name　　　　查找属于用户 name 的文件

-type [fdlcb]　　　　查找指定类型的文件（例如。d 代表目录，l 代表连接）

-size [+/-]n[ck]　　　　查找指定大小的文件（例如，+10k 表示大于 10KB）

-inum number　　　　查找指定 inode 号的文件（硬连接）

只要知道需要查找的文件的任何属性，就可以方便地使用适当的 find 参数来查找。一旦文件被查到以后，它就可以作为一个参数提交给任何 Linux 命令或 shell 脚本运行。

选项-name 支持 shell 的通配符（*，?和[ ]），如果文件名中包含这些字符，一定要记得使用双引号把它括起来，以免 shell 自动把它展开成文件名或者作为参数替换掉。

在线帮助书介绍了更多有关 find 命令的可选参数，它们支持更强大查找规则。在实际使用中， find 并不用来查找文件（一般使用 whereis），而是用来在文件系统中搜寻满足选择规则的文件，然后根据结果运行一个命令。其中一个用处是查找所有最后使用日期在某个指定时间之前的文件，然后把它们移动到一个存档目录中。

这些操作可以是：

-print	在标准输出中打印文件名
-exec command {} \;	对找到的文件执行指定的命令
-ok command {} \;	在执行命令之前请求确认

2.4.6.2 locate

locate 的格式：

```
locate pattern
```

其中 pattern 是匹配的模式。用 locate 命令，用户可以查看和给定模式向匹配的每一个文件和目录。例如，要查找名字中包含 finger 的所有文件，只要输入：locate finger 即可。

命令 locate 通过数据库查找文件名或目录名中包含单词 finger 的文件名或目录名。类似于文件名为 finger.txt 或 pointerfinger.txt 的文件，目录名为 /fingerthumbnails/的目录都会被搜索出来。如果想对 locate 有更多的了解，请查阅 locate 的手册。

2.4.6.3 which，whereis，whatis

2.4.6.3.1 which

命令 which 的格式为：

```
which command
```

命令 which 将会给出该二进制文件、可执行文件或 shell 命令的位置。例如，输入命令

```
which gedit
```

会得到结果/usr/bin/gedit。

2.4.6.3.2 whereis

命令 whereis 的格式为：

```
whereis command
```

下面这个命令可以返回 find 命令的二进制文件位置、源代码位置和手册页位置：

```
whereis find
/usr/bin/find    /usr/share/man/man1p/find.1p.gz /usr/share/man/man1/find.1.gz
```

2.4.6.3.3 whatis

命令 whatis 的格式为：

```
whatis command
```

这个命令可以得到关于 command 手册页中的信息。如果执行命令

whatis lp

就可以得到如下结果：

```
lp                   (4) - line printer devices
lp(lp-cups) (1) - print files
```

2.4.7 在 shell 提示下查看文本文件

2.4.7.1 使用 head 命令

head 命令用于显示文件的开始部分。它的格式为：

```
head <filename>
```

默认情况下，head 只显示文件开始部分的前十行。用户可以通过选项来改变显示的行数。

```
head -20 <filename>
```

上面的命令用于显示文件的前 20 行。

2.4.7.2 使用 tail 命令

tail 命令刚好与 head 命令相反，它用于显示文件的末尾部分，这对于查看日志文件是非常有用的。用-f 选项可以让 tail 实时地将文件中的新信息打印到屏幕上。例如，用命令

```
tail –f /var/log/messages
```

可以让 tail 命令实时地将 messages 中的最新信息打印到屏幕上，可以按[Ctrl]-[C]来终止。

2.4.7.3 使用 less 命令

命令 less 的格式是：

```
$ less [options] [name of file to view]
```

使用 less 命令来查看文件时，可以使用数种击键命令，主要的击键命令如下：

击键命令	功能
空格	向下滚动一个屏幕
回车	向下滚动一行
q	中断显示、退出
/<search pattern>	从当前屏幕开始，正向搜索“search pattern”。
n	重复搜索操作
d	向下滚动半屏
h	显示帮助信息
w	向上滚动一个屏幕
u	向上滚动半个屏幕
y	向上滚动一行

? <string pattern>	从当前屏幕开始，逆向搜索“search pattern”。
N	从当前屏幕开始，重复执行前一次的逆向搜索操作
m	给出详细提示（与 more 类似），屏幕上最后一行的位置将以它在文件中的百分比表示。缺省情况下，less 的提示是冒号“:”。
M	给出的提示比 m 更详细

表 2-6 less 中常用的命令

例如，如果向显示文件/etc/X11/xinit/xinitrc 的内容，可按下述方式使用命令 less：

```
$ less /etc/X11/xinit/xinitrc
userresources=$HOME/.Xresources
usermodmap=$HOME/.Xmodmap
sysresources=/etc/X11/xinit/Xresources
sysmodmap=/etc/X11/xinit/Xmodmap
if [-f $sysresources ]; then
xrdb -merge $sysresources
fi
if [ -f $sysmodmap ]; then
xmodmap $sysmodmap
fi
if [ -f $userresources ]; then
/etc/X11/xinit/xinitrc 1/89 30%
```

如果在一个屏幕上仅显示了文件的部分内容，在屏幕的下方将出现一个状态行，在该行上将显示类似“/etc/X11/xinit/xinitrc 1/89 30%”的内容，它表示的是，已经显示的内容在文件中的百分比。当与-m 选项一起使用命令

less 时，就会显示百分比。

2.4.7.4 使用 more 命令

命令 more 是命令 less 的较早版本，其特性也不如 less 丰富，more 命令的格式是：

```
$ more [options] [name of file to view]
```

对于 more 命令，缺省设置是给出“已显示内容的百分比”。

2.4.7.5 使用 cat 命令

如果你打算查看文本文件的内容，可以使用命令 cat、less 和 more。命令 cat 的格式是：

```
$ cat [options] [name of file to view]
```

常用的选项是：

-n	显示行号

表 2-7 cat 常用的选项

例如，如果希望显示文件/etc/lilo.conf 的内容，可以按下述方式使用命令 cat：

```
$ cat -n /etc/lilo.conf
1 boot=/dev/hda
2       map=/boot/map
3       install=boot/boot.b
4 prompt
5 lba32
6       imeout=50
7       default=linux
```

```
8       image=boot/vmlinuz
9               label=linux
10              root=/dev/hda6
11              initrd=/boot/initrd
12              read-only
```

2.4.7.6 使用 grep 命令

如果打算搜索文本文件中的文本字符串，应使用命令 grep，该命令的格式是：

```
$ grep [options] [string pattern for search] [target files]
```

该命令的常用选项包括：

-i	在搜索过程中，忽略大小写字符之间的区别
-l	不同于常规的搜索结果，仅列出文件的名称
-n	显示行的号码
-x	仅搜索与整个“string pattern”行相匹配的结果。

表 2-8 grep 常用的选项

例如，如果打算在/etc/lilo.conf 下搜索包含字符串“boot”的所有文件，可以按下述方式使用命令 grep：

```
$ grep -n boot /etc/lilo.conf
1:boot=/dev/hda
2:map=/boot/map
3:install=/boot/boot.b
8:image=/boot/vmlinuz
11: initrd=/boot/initrd
```

其中，-n 选项可以在显示出的搜索结果上添加行号。

2.4.8 shell 中的操作信息

从 shell 的角度看，其信息可以分为三类：标准输入、标准输出和标准出错。简单地说，标准输入就是用户通过键盘输入给 shell 的信息，比如说用户输入的命令、文件名等。标准输入就是 shell 在执行用户的命令后打印到屏幕上的基本信息。而标准出错则是当 shell 在发现有错误时打印到屏幕上的出错信息。

这一部分我们将简单地介绍对标准 I/O 信息的操作。

2.4.8.1 管道

管道是用符号“|”来表示的。它可以将一个进程的标准输入连接到另一个进程的标准输入。对命令 cat，如果用户执行

```
cat filename
```

则 shell 会将文件 filename 的内容一次性全部打印到屏幕上。如果文件很长，需要翻很多页，则前面的部分用户就看不到了。如果用命令

```
cat filename | less
```

则 shell 会将 cat 的输出作为 less 的输入。这样如果遇到长文件，就不会出现屏幕上不停翻页，直到把文件显示完的情况了，用户可以用上下箭头在文件中向前移动或向后移动。

2.4.8.2 重定向

所谓重定向就是改变标准输入的来源或改变标准输出的去向。符号“>”用于重定向标准输出。将“>”置于 cat 命令（或其他会向标准输出打印信息的命令）之后，cat 输出的信息就会被重定向到跟在“>”之后的文件内。

cat 命令会将用户输入的内容回显到屏幕上。这些回显的内容是 cat 命令的标准输出。要想重定向输出到一个文件（比如说文件 foo.txt）中，只要在 shell 提示中输入 cat > foo.txt，按回车，然后输入几行文字，最后按[Ctrl]-[D]

退出 cat 程序。图 2-28 是一个重定向的例子。

```
File  Edit  View  Terminal  Tabs  Help
[user@dhcp59-199 ~]$ cat > foo.txt
line 1
line 2
line 3
[user@dhcp59-199 ~]$
```

图 2-28 重定向到文件

```
File  Edit  View  Terminal  Tabs  Help
[user@dhcp59-199 ~]$ cat > foo.txt
line 1
line 2
line 3
[user@dhcp59-199 ~]$ cat > bar.txt
line A
line B
line C
```

图 2-29 重定向到第二个文件

图 2-29 是重定向到另外一个文件的例子。

```
File  Edit  View  Terminal  Tabs  Help
[user@dhcp59-199 ~]$ cat > foo.txt
line 1
line 2
line 3
[user@dhcp59-199 ~]$ cat > bar.txt
line A
line B
line C
[user@dhcp59-199 ~]$ cat foo.txt bar.txt > example1.txt
[user@dhcp59-199 ~]$
```

图 2-30 连接两个文件

图 2-30 示范了 cat 的连接功能。cat 将 foo.txt 追加到 bar.txt 之后，然后重定向到 example.txt。

```
File  Edit  View  Terminal  Tabs  Help
[user@dhcp59-199 ~]$ cat > foo.txt
line 1
line 2
line 3
[user@dhcp59-199 ~]$ cat > bar.txt
line A
line B
line C
[user@dhcp59-199 ~]$ cat foo.txt bar.txt > example1.txt
[user@dhcp59-199 ~]$ cat example1.txt
line 1
line 2
line 3
line A
line B
line C
[user@dhcp59-199 ~]$
```

图 2-31 example1.txt 中的内容

图 2-31 演示了用 cat 显示 example1.txt 中的内容。

2.4.8.3 追加到标准输出

符号“>>”表示追加到标准输出。即将输出的内容追加到被定向的文件末尾，而不是将被定向的文件全部覆盖。图 2-32 演示了用 cat 命令将 bat.txt 追加到 foo.txt。

```
File  Edit  View  Terminal  Tabs  Help
line 1
line 2
line 3
[user@dhcp59-199 ~]$ cat > bar.txt
line A
line B
line C
[user@dhcp59-199 ~]$ cat foo.txt bar.txt > example1.txt
[user@dhcp59-199 ~]$ cat example1.txt
line 1
line 2
line 3
line A
line B
line C
[user@dhcp59-199 ~]$ cat bar.txt >> foo.txt
[user@dhcp59-199 ~]$ cat foo.txt
line 1
line 2
line 3
line A
line B
line C
[user@dhcp59-199 ~]$
```

图 2-32 将 bar.txt 追加到 foo.txt 末尾

2.4.8.4 重定向标准输入

符号“<”表示重定向标准输入。用户可以用重定向标准输入指定一个文件作为输入的内容。图 2-33 是将文件 foo.txt 重定向标准输入的一个例子。

```
File  Edit  View  Terminal  Tabs  Help
[user@dhcp59-199 ~]$ cat example1.txt
line 1
line 2
line 3
line A
line B
line C
[user@dhcp59-199 ~]$ cat bar.txt >> foo.txt
[user@dhcp59-199 ~]$ cat foo.txt
line 1
line 2
line 3
line A
line B
line C
[user@dhcp59-199 ~]$ diff foo.txt example1.txt
[user@dhcp59-199 ~]$ cat < foo.txt
line 1
line 2
line 3
line A
line B
line C
[user@dhcp59-199 ~]$
```

图 2-33 重定向标准输入

2.4.9 使用多个命令

linux 允许用户一次输入多个命令。命令之间需要用分号“；”分隔。例如，要在当前目录下创建目录 doc，然后再将当前目录下的文件 doc.txt 移动到目录 doc 下，就可以用下面这一条命令完成：

```
mkdir doc; mv doc.txt doc
```

2.4.10 所有权和权限

作为一个普通用户，如果您想进入根用户的主目录，只要执行命令 cd /root 就可以了，但屏幕上会显示如下出错信息：

```
-bash: cd: /root/: Permission denied
```

这是因为普通用户没有对根用户主目录的访问权限。Linux 像 Unix 一样是一个多用户的系统。Linux 也用文件访问权限作为防止系统被恶意篡改的

方法之一。

文件和目录都是属于它们的创建者的。如果您在您的主目录下创建了文件 foo.txt，那么这个文件就属于您。这就意味着您可以指明谁可以查看该文件的内容，谁可以修改这个文件，以及谁可以执行这个文件。权限就是由读、写、执行这三部分组成的。如果某一个用户的帐户在被创建的时候就被加入了和您同一个组，那么您可以通过指明同组成员对文件 foo.txt 的权限来指明该用户对文件 foo.txt 的权限。您可以用 ls 加-l 选项查看文件或目录的权限。图 2-34 给出了一个查看文件 sneakers.txt 权限的例子。第一列中显示的就是文件的权限，一共有 10 个字符。其中左边第一个字符表示类型（-表示普通文件，d 表示目录，l 表示符号连接）。剩下的 9 个字符可以分为三部分，每部分包含三个字符，从左到右分别表示读权限、写权限、执行权限（r 表示读权限，w 表示写权限，x 表示执行权限，-表示未指明）。左边三个字符为第一部分，表示文件的拥有者，中间三个字符表示同组成员，右边三个字符表示其他用户。图 2-34 中的显示结果表明 sneakers.txt 是一个普通文件，文件的拥有者对它有读、写权限，文件拥有者的同组成员对它也有读、写权限，其他成员就只有读权限，任何都没有对该文件的执行权限（该文件应该是一个不可执行的文件）。

File Edit View Terminal Go Help

```
[sam@Halloween sam]$ ls -l sneakers.txt
-rw-rw-r--    1 sam      sam           66 Aug 16 14:21 sneakers.txt

[sam@Halloween sam]$
```

图 2-34 显示文件的权限

2.4.10.1 chmod 命令

用户可以用 chmod 命令修改权限。下面通过用 chmod 修改文件 foo.txt 的权限来演示 chmod 的用法。

文件 foo.txt 原来的权限为（用 ls –l foo.txt 得到）：

```
-rw-rw-r--    1 user user    150 Mar 19 08:08 foo.txt
```

输入命令：

```
chmod o+w foo.txt
```

表示为其他用户添加写权限。执行 ls –l foo.txt 后，可得到显示结果：

```
-rw-rw-rw-    1 user user    150 Mar 19 08:08 foo.txt
```

输入命令：

```
chmod go-rw foo.txt
```

表示取消同组成员和其他成员对该文件的读、写权限。执行 ls –l foo.txt 后，可得到显示结果：

```
-rw-------    1 user user    150 Mar 19 08:08 foo.txt
```

下面给出 chmod 中参数和选项的列表：

- 身份

u－拥有者

g－拥有者的同组成员

o－其他成员（不包含拥有者和拥有者的同组成员）

a－所有成员

- 权限

r－读权限

w－写权限

x－执行权限

- 操作

＋－增加权限

-－去除权限

＝－指明确切的权限

下面给出一些参数和选项的使用示例：

- g+w－为拥有者的同组成员增加写权限
- o-rwx－去除其他成员的读、写、执行权限
- u+x－为拥有者添加执行权限
- a+rw－为所有成员增加读、写权限
- ug+r－为拥有者及其同组成员增加读权限
- g=rx－将拥有者同组成员的权限设置程读和执行

用户还可以用-R 选项对目录以及目录下的所有文件和子目录递归执行 chmod 命令。

2.4.10.2 用数字修改权限

访问权限还可以用数字来表示。例如：

```
-rw-rw-r--      1 user user       150 Mar 19 08:08 foo.txt
```

对于用右边 9 个字符表示的三个部分，每一个部分都可以用数字表示：

- r=4
- w=2
- x=1
- -=0

将这些数字加在一起就表示某一个部分的权限。比如说，您想要表示读和写权限，那么可以用 6 表示，因为 4（read）＋2（write）＝6。如果您想

为将文件 foo.txt 的权限设置成-rw-r--r--，则可以通过执行下面命令来实现：

```
chmod 644 foo.txt
```

现在如果执行命令：

```
ls –l foo.txt
```

则可以看到如下显示：

```
-rw-r--r--     1 user user     150 Mar 19 08:08 foo.txt
```

2.5 连接因特网

GTES10 为用户提供了多种连接到因特网的工具。一般连接到因特网的方式有以下几种：

- ISDN 连接：ISDN（Integrated Services Digital Network 的缩写）连接是一种用高速、高质量电话线连接到因特网的方式。与用模拟信号的调制解调器连接方式不同的是 ISDN 所使用的专用电话线要由电话公司来安装。

调制解调器连接：调制解调器连接就是用普通电话线连接到因特网。数字信号被转换成模拟信号后在通过电话线传输到因特网。

- 无线连接：无线连接是用无线连接点（WAP）或者带无线网卡的端对端网络连接到因特网的。
- xDSL 连接：xDSL（Digital Subscriber Line 的缩写）是通过高速电话线连接到因特网的。它包括几种不同的 DSL，其中包括 ADSL, IDSL 和 SDSL。互联网配置向导所用的术语 xDSL 指的是上面提到的任何一种 DSL。
- 以太网连接：有些 xDSL 和电缆调制解调器通过以太网建立连接。xDSL 或电缆调制解调器之间和以太网卡通进行通信，网卡再依次和您的 ISP 进行通信。

这一部分我们将详细介绍如何用调制解调器建立连接。建立其他类型连接的步骤与建立调制解调器的步骤差不多。在建立连接之前，您应该检查一下您的 ISP 提供的说明信息，其中包括：

- 拨号使用的电话号码（如果您使用调制解调器连接）。

- 您帐户的登录名和密码（如果您使用调制解调器或 Xdsl）。
- 网关地址。
- 域名服务器（DNS－Domain Name System 的缩写）地址。

2.5.1 互联网配置向导

只要在主菜单中选择“系统工具->互联网配置向导”或者是在命令行方式下输入命令：

```
internet-druid
```

就可以打开如图 2-35 所示的互联网配置向导。互联网向导会一步一步指导您建立新的互联网连接。

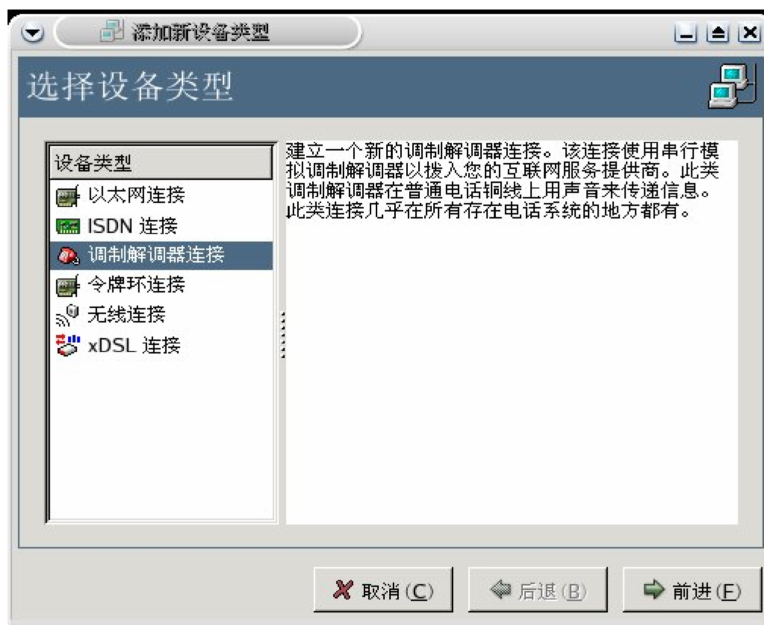


图 2-35 互联网配置向导

2.5.2 创建拨号连接

建立拨号连接要求您用调制解调器通过向一个电话号码拨号，然后连接到您的因特网服务提供商（ISP）。这就要求您的计算机上必须具备调制解调器。

创建新的调制解调器连接步骤：

第 1 步：在主菜单中选择“系统工具->互联网配置向导”，以打开互联网配置向导。

第 2 步：如果系统提示要输入根用户密码，则输入密码后按回车键。

第 3 步： 在左侧选择设备类型中选择“调制解调器连接”，点击“前进”按钮。则系统会自动探测调制解调器，然后会以打开“添加新设备类型”窗口。

第 4 步： 在“添加新设备类型”窗口中有三个下拉式选择框：

- 调制解调器设备：这个菜单中列出了您系统中已经安装的所有调制解调器。您应该从中选择一个，用来建立新连接。
- 波特率：选择您调制解调器的速率。56.6k 的调制解调器速率为 56700。
- 流程控制：如果您的调制解调器是一个安装在您系统上的硬件设备，就在这里选择“硬件”。

选择完上面三个选择框后，点击“前进”按钮，进入下一个窗口“选择提供商”。

第 5 步： 在这个窗口中，您必须填写您的提供商信息。其中包括一下几个区域：

- 前缀：输入您要访问的号码的前缀。例如，如果想拨外线就填“9”，如果想拨长途就填“1”。
- 区号：输入您要访问号码的区号。
- 电话号码：输入要访问的电话号码。
- 提供商名称：输入您提供商的名称。
- 登录名：输入提供商为您创建的登录名。

- 口令：输入您帐户的口令。

填写完上述内容后，点击“前进”按钮，进入下一个窗口“IP 设置”。

第 6 步： 在这个窗口中，您可以选择“自动获取 IP 地址设置”或者“静态设置的 IP 地址”。如果您选择了“静态设置的 IP 地址”，那么您必须自己填写“地址、子网掩码、默认网关地址”这三项。设置完后，点击“前进”按钮，进入下一个窗口“建立拨号连接”。

第 7 步： “建立拨号连接”窗口是最后一个窗口。在这个窗口中会显示您刚才的配置信息：硬件、提供商名称、登录民、电话号码，点击“应用”按钮后就会创建新的连接了。然后会出现“网络配置”窗口。

第 8 步： 在“网络配置”窗口中显示了您所建立的所有连接的列表。

到此为止，建立新的调制解调器连接工作已经完成。

2.5.3 创建高速连接

创建高速连接的步骤和创建调制解调器连接的步骤差步多。您可以使用“DHCP 的方式获取 IP 地址”，只要打开互联网配置向导，选择以太网连接，然后在“配置网络设置”窗口中选中“自动获取 IP 地址设置使用”的单选框即可。

2.5.4 创建无线连接

如果您是用无线（802.11.x）网卡连接到互联网的，那么您必须配置您的无线设备。具体步骤如下：启动互联网配置向导，选择“无线连接”，然后就可以跟着提示一步一步配置了。

2.6 web 浏览器

当您建立了互联网连接后，您就可以上网浏览了。GTES10 为用户提供了多种 web 浏览器。我在前面介绍过 Konqueror，这一部分主要介绍 Firefox。

2.6.1 Firefox



图 2-36 Mozilla Firefox

Firefox 是 mozilla.org 的一部分。Firefox 的特点包括：可以用标签浏览、使用插件、可以对浏览器使用扩展和修改主题。这一部分主要介绍 Firefox 的使用。

如果用户想要获取关于 Firefox 的详细文档，可以访问 Mozilla.org 的提供的资源：

http://www.mozilla.org/support/firefox

http://www.mozilla.org/community

2.6.1.1 使用 Firefox

像其他浏览器一样，Firefox 也有标准的导航工具条、按钮、菜单。导航工具条中包含导航图标、地址栏和搜索区（如下图所示）。



图 2-37 导航工具条

只要在地址栏中输入 URL（Uniform Resource Locator 的缩写），然后按回车，Firefox 就会打开相应的 web 页面。

搜索区用目前最流行的搜索引擎查找与用户输入的关键字想匹配的站点。您可以点击搜索区图标，选择自己喜欢的搜索引擎（如下图所示），然后输入关键字，按回车就可以用您选择的搜索引擎根据刚才输入的关键字进行搜索了。



图 2-38 搜索区

Firefox 还有侧栏，为用户提供了更多便利。在主工具条中选择“查看->侧栏”就可以在看到侧栏中的内容。侧栏中包含书签和历史两项。您可以在书签中选择设置好的书签，或在历史中查看您最近浏览过的网页。

您还可以为经常浏览的站点做一个按钮添加到个人工具条（如下图所示）中。您所要做的操作仅仅是点中地址栏中站点的图标，将其拖到个人工具

条中，然后放开即可。如果下次想要访问该站点，您只要点击这个新生成的按钮即可。



图 2-39 个人工具条

2.6.1.2 标签

Firefox 为用户提供了标签的功能。用户可以在同一个 Firefox 窗口中打开多个标签。每个标签可以单独打开一个站点。打开新标签的步骤是在菜单中选择“文件->新建标签页”，快捷方式为[Ctrl]-[T]。



图 2-40 打开的标签

2.6.1.3 插件

插件为Firefox提供了扩展的功能。您可以自己下载插件，然后自己安装。您可以在 http://channels.netscape.com/ns/browsers/plugins.jsp找到全部插件的列表。

2.6.1.4 扩展和主题

Firefox 有许多扩展和主题。扩展是一些 applet（小的 java 程序）。它们为 Firefox 提供了许多附加的功能。您可以在菜单中选择“工具->扩展”，来获取更多的扩展。

主题允许您修改 Firefox 的外观风格。您可以在菜单中选择“工具->主题”，

然后在弹出的窗口选择自己喜欢的主题，也可以在该窗口中点击“获取更多主题”从网上下载主题。

2.7 电子邮件应用程序

电子邮件客户端是常用的应用程序之一。GTES10 提供的电子邮件客户端程序有 Evolution 和 Thunderbird。它们都是图像界面客户端，但各有特点。您可以根据自己的喜好进行选项。这一部分我们将介绍这两种电子邮件客户端的用法。

在启动电子邮件客户端之前，您应该已经拥有一个合法的电子邮件帐户，并且还需要知道以下信息：

- 您的电子邮件地址：您用来收发电子邮件的帐户，即形如<yourname>@<example.com>的字符串。
- 接收邮件的服务器类型：为了能收取电子邮件，您必须知道您的 ISP 所用的接收邮件服务器类型，即 POP 或 IMAP。
- 接收邮件的地址：为了能接收电子邮件，您必须知道您的 ISP 所用的 POP 或 IMAP 服务器的地址，即形如 mail.example.com 的字符串。
- 发送邮件的服务器类型（SMTP）：简单邮件传输协议 SMTP（Simple Mail Transfer Protocol 的缩写）是用于在两个邮件服务器之间发送邮件的协议。大部分电子邮件系统都用 SMTP 在互联网上发送电子邮件。而且电子邮件客户端向服务器发送电子邮件用的也是 SMTP。

下面我们将演示两种电子邮件客户端配置的方法。

2.7.1 Evolution

Evolution 不仅仅是一个邮件客户端。它除了拥有标准邮件客户端所具备的特性（例如：邮箱管理、自定义过滤器、快速搜索等）外，还提供了如日历之类的其他额外的功能。

启动 Evolution 的步骤是在主菜单中选择“因特网->电子邮件”。

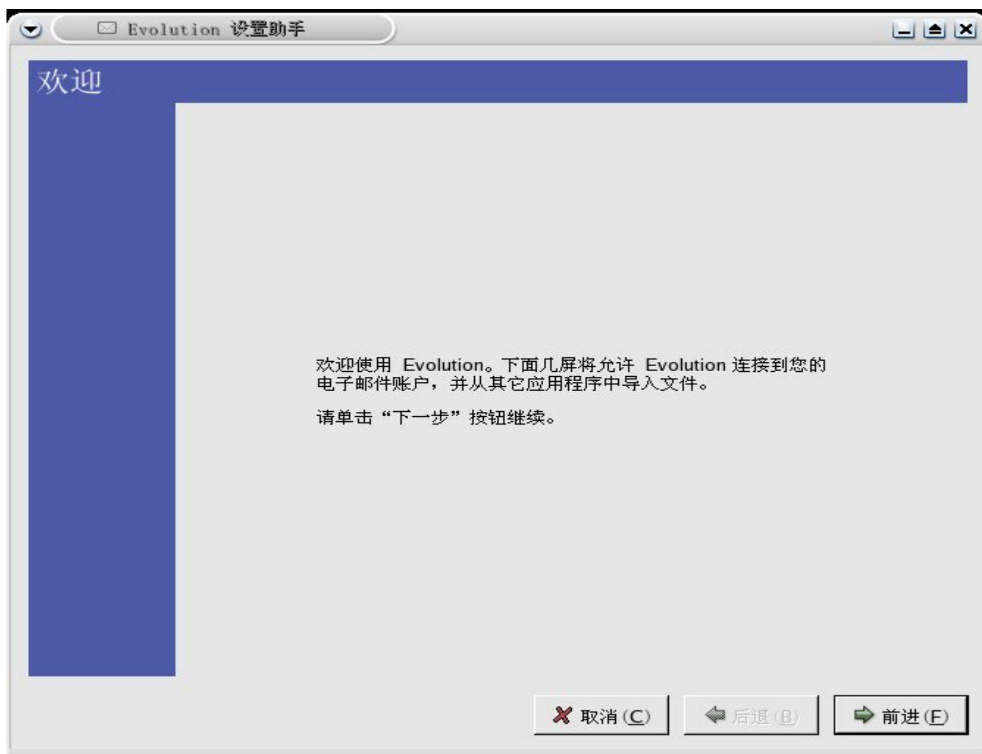


图 2-41 Evolution 欢迎窗口

第一次启动 Evolution 的时候会出现如图 2-41 所示的欢迎窗口。您可以在这个窗口的引导下配置您的电子信箱。

当用户配置完自己的帐户后，就会出现如下图所示的 Evolution 主界面。

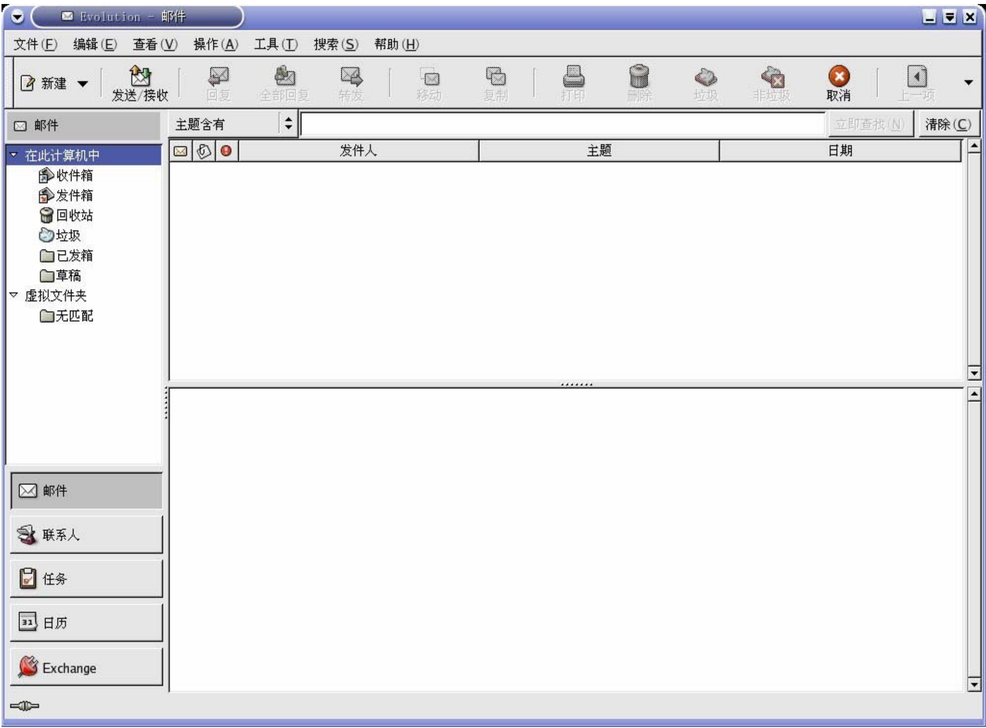


图 2-42 Evolution 主界面

点击 Evolution 主界面左下方的“邮件”按钮就可以查看收件箱、发件箱、回收站、垃圾、已发箱、草稿这几个文件夹（如图 2-43 所示）。

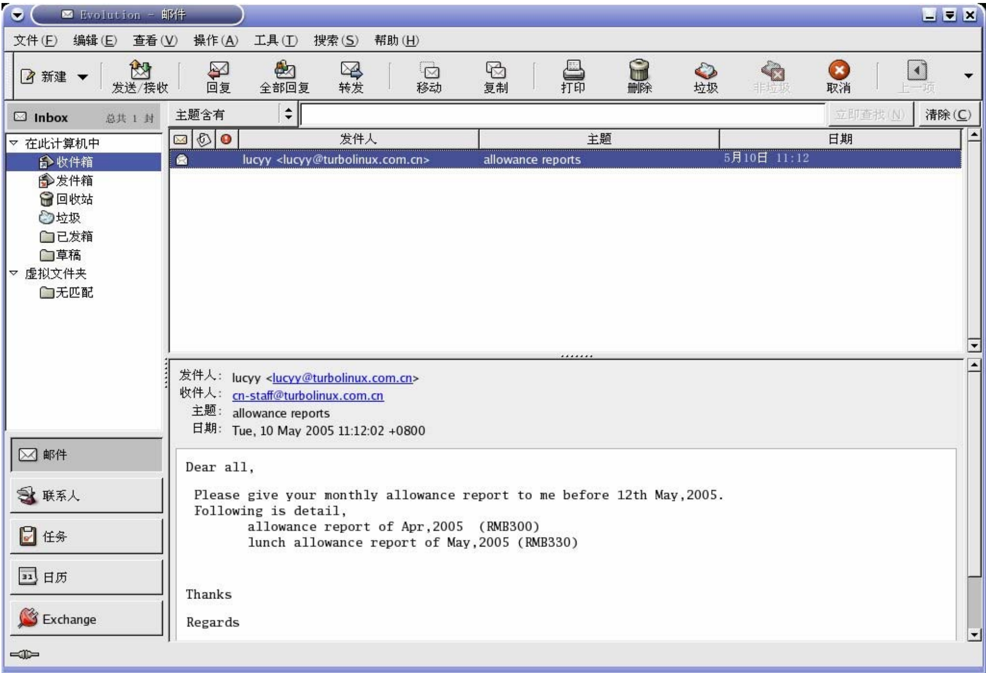


图 2-43 Evolution 收件箱界面

如果要撰写新邮件，可以选择左上角的“新建”下来菜单，然后选择“信件”，在弹出的窗口中就可以编辑您的邮件了。您可以点击“附件”按钮来添加附件，点击“发送”按钮即可将邮件发送出去。

2.7.2 Thunderbird

启动 Thunderbird 的步骤为：选择“主菜单->因特网->Thunderbird Mail”。第一次启动时会出现一个窗口（如图 2-44），问您是否需要导入一个帐户。如果您选择跳过，那么就会出现如图 2-45 所示的创建新帐户界面。您可以根据提示逐步配置自己的帐户。

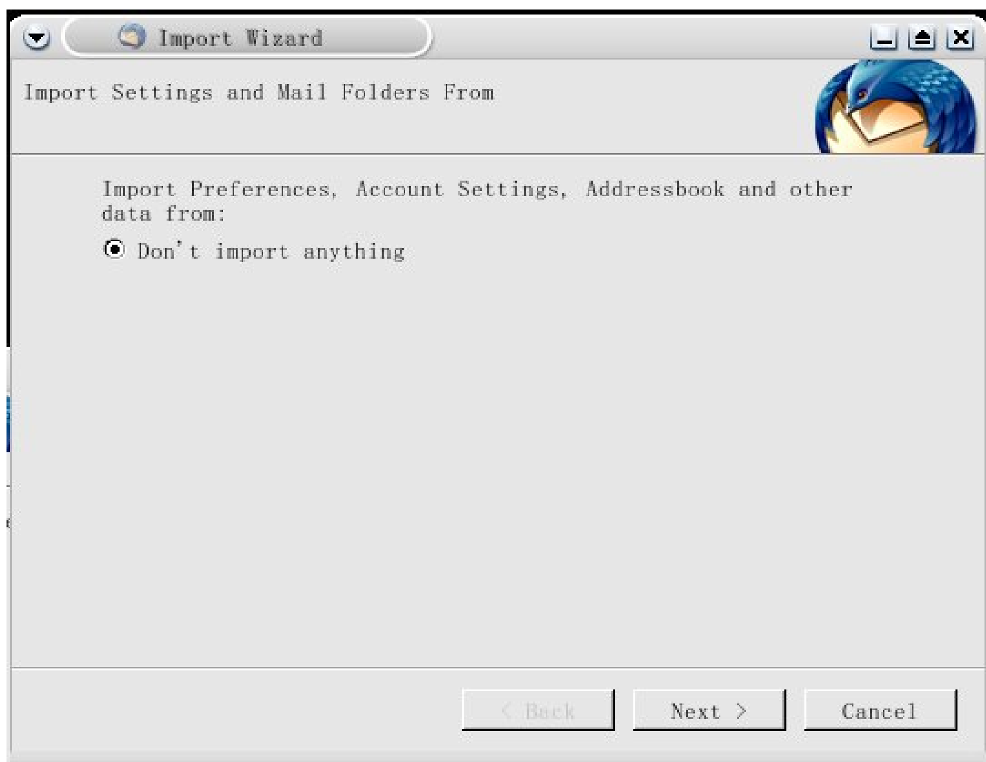


图 2-44 Thunderbird 导入向导

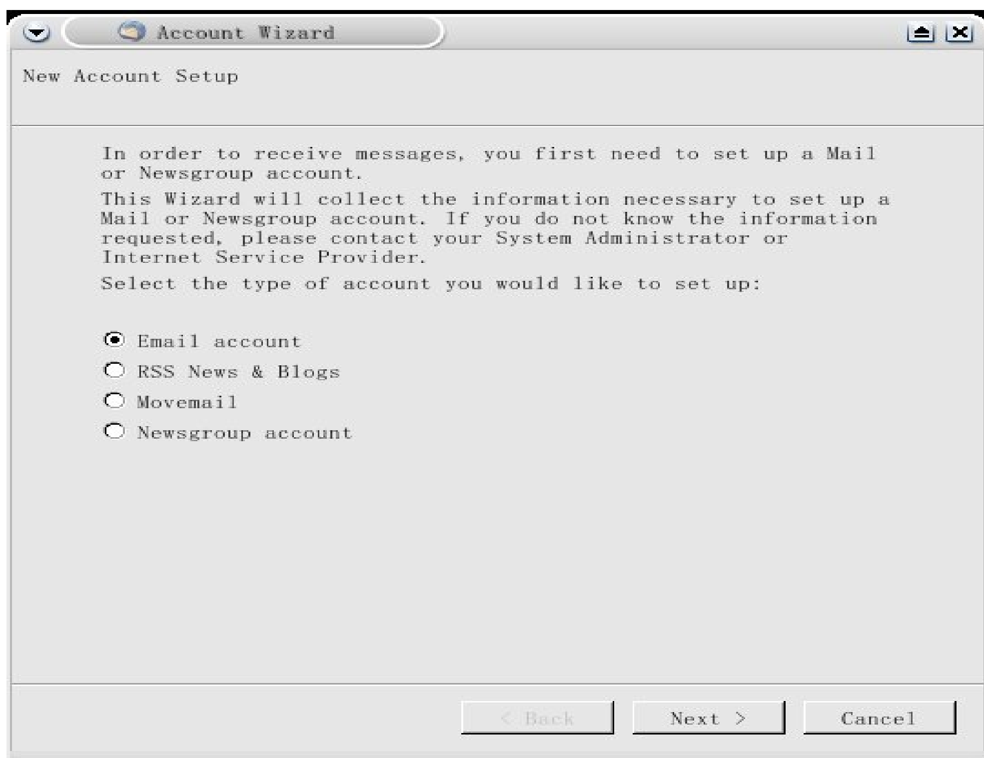


图 2-45 Thunderbird 创建新帐户

新帐户创建完毕后，用户就可以看到如图 2-46 所示的主界面了。

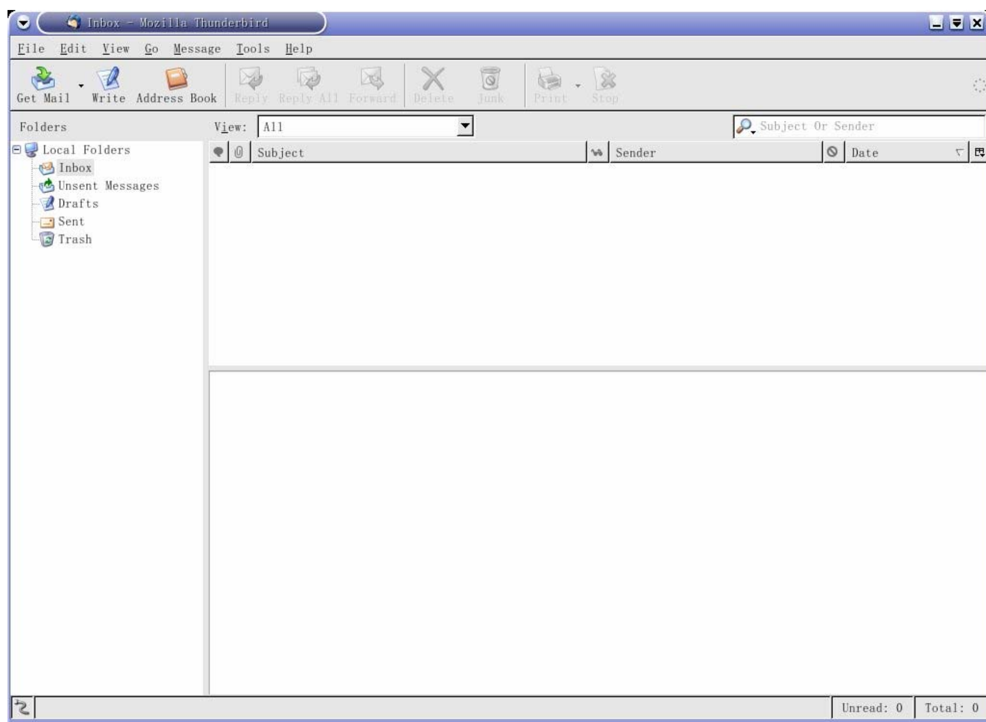


图 2-46 Thunderbird 主界面

“Get Mail”按钮用于收取新邮件。“Write”按钮用于撰写新邮件。如果想在邮件中添加附件，可以在顶部的菜单中选择“File->Attach”，然后根据出现的项进行选择。如果要添加的附件是文件，则可以选择“Files”。

2.8 其他文本工具

2.8.1 文本编辑器

2.8.1.1 vi

vi 是一个命令行方式下的文本编辑器，运行 vi 的时候不需要图形环境。在控制台中输入命令 vi 即可启动 vi。例如想在当前目录下编辑文件 foo.txt，则输入命令：vi foo.txt。vi 是用键盘方式操作的。下面列出少数常用的 vi 命令。

- [i]：用 vi 打开文件后，按[i]键即可进入编辑模式。
- [Esc]：当处于编辑模式时，按[Esc]键即可回到命令模式。
- [w]：按[Shift]-[:]后输入 w，再按回车即可将文件存盘。
- [q]：按[Shift]-[:]后输入 q，再按回车即可退出 vi。如果输入 wq，表示存盘并退出；如果输入 q!，表示不存盘强行退出。
- [!]：强制 vi 执行指定命令。如 q!表示强行退出。

vi 的功能非常丰富。如果想对 vi 有更加详细的了解，请查询 vi 的手册（即 man vi）。

2.8.1.2 Emacs

Emacs 是一个可以使用鼠标的文本编辑器。用户可以自己选择用键盘还是鼠标，所有的命令在两种方式下都可以使用。用户可以在 Emacs 的工具条中选择“Help->Eamcs Tutorial”查看 Emacs 的指南。

2.8.1.3 gedit

gedit 是 GNOME 下的文本编辑器。它对 HTML、C、PHP、Perl 和其他一些编程语言都具有加亮模式。

2.8.1.4 Kate

Kate 是 KDE 下的文本编辑器。它也对多种程序语言都具有加亮度模式。Kate 可以用分隔窗口的方式显示多个文件，还可以在 Kate 窗口内打开终端窗口。

2.8.2 PDF 和 PS 查看工具

GTES10 中可用于查看 PDF 格式文件的工具是 PDF 阅读器。打开 PDF 阅读器的方式为选择主菜单中“编辑与查看->PDF 阅读器”，或者是在 Konqueror 中双击 PDF 文件也可。

用于查看 PS 格式文件的工具是 PostScript Viewer。打开的方式是选择主菜单中“编辑与查看->PostScript Viewer”，或者是在 Konqueror 中双击 PS 文件也可。

2.9 音频、视频和游戏

2.9.1 播放 cd

用户将 cd 放入光驱后，cd 播放器就会自动出现，并且开始播放 cd 上的第一个音轨。如果 cd 播放器的界面没有自动出现，可以选择“主菜单->多媒体->KsCD”来启动它。



图 2-47 cd 播放器界面

2.9.2 播放数字音频文件

由于数字音频的音质非常好，所以越来越受到用户的喜爱。GTES10 为用

户提供了功能强大的数字音频播放器：XMMS（X Multimedia System 的缩写）。它可以播放包括 mp3、Ogg、RIFF 在内的多种格式的数字音频文件。



图 2-48 XMMS 界面

启动 XMMS 的方式是选择“主菜单->多媒体->音频播放器”。如果想在命令行方式下启动 XMMS，则只需要输入 xmms，然后按回车即可。

使用 XMMS 的方式也很简单。只要点击按钮，就会出现如图 2-49 所示的窗口。您可以 files 框中选择要播放的文件，添加倒 XMMS 的播放列表中。

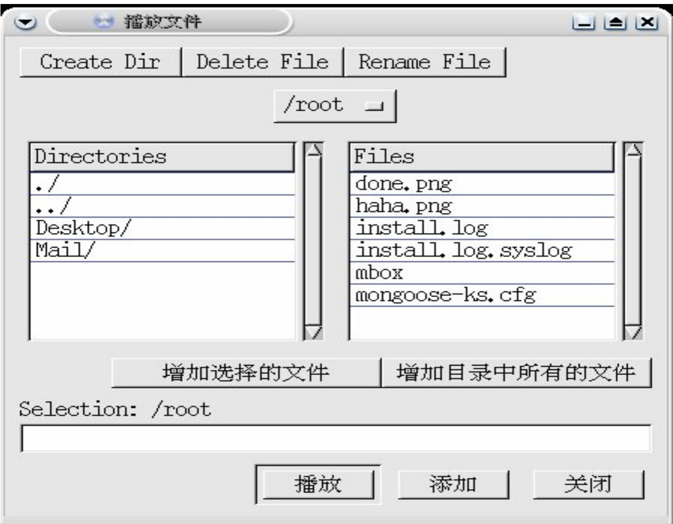


图 2-49 XMMS 加载文件窗口

2.9.3 解决声卡故障

如果您系统上的声卡不能发出声音，您可以用运行声卡配置工具重新配置您的声卡。启动声卡配置工具的方式为选择“主菜单->系统设置->声卡检测”。出现如图 2-50 的窗口后，点击播放测试声音进行声卡检测。



图 2-50 声卡配置工具

如果声卡配置工具不管用，您还可以手工配置声卡。手工配置声卡就需要编辑文件/etc/modules.conf，将声卡所需的内核模块添加到文件中。下面是一个例子：

```
alias sound sb

alias midi opl3

options opl3 io=0x388

options sb io=0x220 irq=7 dma=0,1 mpu_io=0x300
```

2.9.4 解决显卡故障

显卡配置的工作是在系统安装过程中完成的。但是如果您想修改系统安装过程中的配置，可以用显卡配置工具进行修改。启动显卡配置工具的方式为选择“主菜单->系统设置->更多系统设置->显示”。

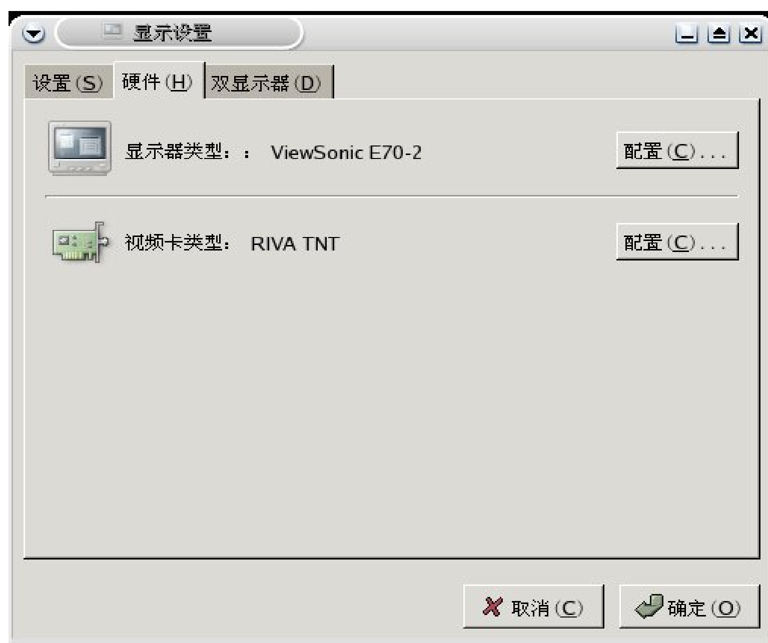


图 2-51 显卡配置工具

如果想对显示器和显卡进行配置，点击“硬件”按钮，然后就可以点击配置进行硬件选择了（如图 2-51 所示）。

2.10 图片

2.10.1 保存图片

从 web 页面上获取图片的方式为右键点击图片，选择图片另存为。由于版权问题，有些网站会禁止用户将图片另存到本地。从 CD 或其他移动介质上获取图片的方式为选中图片文件，先拷贝，然后粘贴到目标地址。

2.10.2 查看图片

查看图片的方法有多种。最普通的方式是在 Konqueror 中双击图片文件，图片就会显示在 Konqueror 窗口中。

还可以用 GIMP 查看图片。启动 GIMP 的方式为点击"主菜单->图像->The GIMP"。第一次启动的时候会有一个安装过程，只要点继续就可以了。一旦安装完毕，可以在 GIMP 中选择"文件->打开"来选择打开的图片文件。

2.10.3 用 GIMP 编辑和创建图片

对已有图片的修改比较简单。首先获取原始图片，可以从网上找，也可以从其他地方拷贝到机器上。然后在 GIMP 中打开图片文件（上一节已经提到过）。对图片的编辑方式一般有一下几种：

- 剪裁图片

第 1 步 用 GIMP 打开文件。

第 2 步 右键点击图片，选择"工具->变换工具->裁减和改变大小"。

第 3 步 左键点击并拖拽鼠标，用一个大小适合的框将图片框起来。

第 4 步 在弹出的对话框中点击剪裁按钮。

第 5 步 如果您觉得对结果不满意，可以按[Ctrl]-[Z]取消刚才的操作。

- 旋转图片

第 1 步 用 GIMP 打开文件。

第 2 步 右键点击图片，选择"图像->变换"，然后在出现的选项中进行选择。

第 3 步 如果您觉得对结果不满意，可以按[Ctrl]-[Z]取消刚才的操作。

- 在图片中添加文本

第 1 步 用 GIMP 打开文件。

第 2 步 右键点击图片，选择"工具->文字"，左键在图片中点击要输入文字的起始位置。

第 3 步 在弹出的框中输入文字。

第 4 步 点击关闭，就可以看到您输入的文字被添加到图片中了。

第 5 步 如果您觉得对结果不满意，可以按[Ctrl]-[Z]取消刚才的操作。

- 用过滤器

第 1 步 用 GIMP 打开文件。

第 2 步 右键点击图片，选择“滤镜”，选择一个可选的过滤器。

第 3 步 在选中的过滤器中再选择一个出现的选项。

第 4 步 在出现的对话框中点击确定按钮。

第 5 步 如果您觉得对结果不满意，可以按[Ctrl]-[Z]取消刚才的操作。

创建新图片的步骤为：启动 GIMP，选择“文件->新建”，在弹出的对话框中填写好图像大小、图像类型、填充类型后点击确定，然后就可以在弹出的图像编辑窗口中利用各种工具编辑您的图像了，并将其保存就可以了。

2.11 软盘和 CD-ROM

2.11.1 软盘磁盘

2.11.1.1 挂载和卸载软盘

2.11.1.1.1 手工挂载软盘：

第 1 步 将软盘插入软驱。

第 2 步 在命令行中输入

```
mount /medie/floppy
```

可以看到软驱指示灯开始闪烁。

第 3 步 通过访问目录/medie/floppy 就可以访问软盘了。

2.11.1.1.2 用 Konqueror 挂载软盘

第 1 步 将软盘插入软驱。

第 2 步 在桌面上双击主文件夹图标。

第 3 步 在出现的 Konqueror 窗口左侧框中点击设备图标。

第 4 步 在右边主窗口中双击软盘图标即可打开软盘。

2.11.1.1.3 手工卸载软盘

在命令行中输入

```
umount /media/floppy。
```

2.11.1.1.4 用 Konqeror 卸载软盘

第 1 步 在桌面上双击主文件夹图标。

第 2 步 在出现的 Konqueror 窗口左侧框中点击设备图标。

第 3 步 在右边主窗口中右键点击软盘图标，选择“卸载”。

2.11.1.2 格式化软盘

2.11.1.2.1 用 KFloppy 格式化软盘

第 1 步 将软盘插入软驱。

第 2 步 启动 KFloppy：“主菜单->实用工具->KFloppy”。

第 3 步 在出现的 KFloppy 窗口中选择软驱、大小、文件系统，点击“格式化”按钮。

第 4 步 点击“退出”按钮。

2.11.1.2.2 手工格式化软盘

手工格式化的命令为 mke2fs。它只能将软盘格式化成 ext2 格式。假设软盘被插入到第一个软驱中，则执行命令

```
/sbin/mke2fs /dev/fd0
```

即可。如果软盘是在第二个软驱中则需执行命令

```
/sbin/mke2fs /dev/fd1。
```

其他情况也类似。

2.11.2 CD 和 DVD-ROM

2.11.2.1 用文件管理器访问 CD-ROM 和 DVD-ROM

GTES10 的桌面上一个光盘的图标。将 CD（或 DVD）放入光驱，双击该图标后会出现 Konqueror 的窗口，而 CD（或 DVD）上的内容就显示在 Konqueror 中。

2.11.2.2 在 shell 提示下访问 CD-ROM 和 DVD-ROM

shell 提示下访问 CD-ROM 和 DVD-ROM 的步骤如下：

第 1 步：将 CD（或 DVD）插入光驱。

第 2 步 打开一个终端窗口。

第 3 步 执行命令

```
mount /media/cdrom
```

第 4 步 进入目录/media/cdrom 即可访问 CD（或 DVD）。

2.11.3 刻录 CD

2.11.3.1 用 X-CD-Roast 刻录 CD

启动 X-CD-Roast 的方式为："主菜单->系统工具->CD Writer"。

2.11.3.2 用命令行工具刻录 CD

在命令行方式下刻录 CD，首先要将想刻到 CD 上的数据收集起来，制作成一个 ISO9660 格式的映象。如果想要将目录/home/joeuser 下除子目录/home/joeuser/junk 外的所有数据制作成一个名为 backup.iso 的 ISO9660 映象（注意 ISO9660 映象的大小不能超过一张 CD 的容量），可以执行如下命令：

```
mkisofs -o backup.iso -x /home/joeuser/junk/ -J -R -A -V -v /home/joeuser/
```

参数-o 表示输出的 ISO9660 映象名，-x 表示排除掉指定目录。详细参数请参考 mkisofs 手册（man mkisofs）。

制作完 ISO9660 映象后就可以用命令 cdrecord 将其刻录到 CD 上了。将 backup.iso 刻录到 CD 上的命令如下：

```
cdrecord -v -eject speed=4 dev=0,3,0 backup.iso
```

speed 表示刻录的速度为 4 速，dev=0,3,0 表示刻录机的设备地址，-eject 表示刻录完毕后弹出 CD。详细参数请参考 cdrecord 手册（man record）。

2.11.4 USB 盘

2.11.4.1 挂载 USB 盘

将 USB 盘插到 USB 口上后，GTES10 会在自动创建目录/media/usbdisk。如果系统没有创建该目录，应该手工创建。

手工挂载 USB 盘的步骤是：打开一个终端窗口，然后输入命令

```
mount /dev/sda1 /media/usbdisk
```

用 Konqueror 挂载 USB 盘的步骤是：打开 Konqueror，在左边窗口选择“设备”，然后可以在右边窗口看到 USB 盘的图标，双击该图标或者右键点击该图标，选择挂载都可以将 USB 盘挂载到系统上。

2.11.4.2 访问 USB 盘

USB 盘挂载到系统上后，可以在终端窗口中输入 cd /media/usbdisk，进入挂载的目录，或者在 Konqueror 下先在左边窗口选择设备，双击在右边窗口出现的图标即可访问 USB 盘。

2.11.4.3 卸载 USB 盘

在 Konqueror 中卸载 USB 盘的方式为：右键点击 USB 盘图标，选择“卸载”。手工卸载 USB 盘的方式为：在终端输入命令

```
umount /media/usbdisk
```

2.12 常见问题

2.12.1 本地登录和口令

问题：当安装完 GTES10 后，在系统启动时系统提示“it needs a localhost login and password.”。这是怎么回事？

如果您没有设置您的主机名，也没有从网络获取主机信息，那么 GTES10 会将您的主机名设置为默认值－localhost.localdomain。

2.12.2 忘记了根用户口令

问题：忘记了根用户的口令该怎么办？

如果忘记了根用户口令，您可以以单用户模式登录到系统，然后重新创建根用户口令。如果您用 GRUB 引导系统的，那么可以有下面的方式进入单用户模式：

第 1 步 在 GRUB 的引导菜单中，用上下箭头选择要引导的系统，按[A]键进入 append 模式。

第 2 步 屏幕上显示如下：

```
grub append> ro root=LABEL=/
```

第 3 步 在 ro root=LABEL=/后添加单词“single”，注意“single”和前面字符串之间必须要有空格，添加完“single”后屏幕显示如下：

```
ro root=LABEL=/ single
```

第 4 步 按回车键后，系统开始引导启动。等系统启动完毕后出现 shell 提示，如下：

```
sh-2.05b#
```

第 5 步 在 shell 提示后输入命令 passwd root 即可重新创建根用户口令。

2.12.3 忘记了普通用户口令

问题：忘记了普通用户的口令，如何重新创建？

在 GTES10 中，用户口令是存放在加密的文件中的，用户无法看到它的明文。如果您忘记了您的用户口令，那么就必须重新创建一个。

如果在登录时候意识到忘记了口令，那么您可以用用根用户登录，然后用命令 passwd username 为自己的帐户创建一个新口令（其中 username 是您的用户名）。等到下一次登录的时候，您就可以使用新口令。

2.12.4 更改口令

问题：如何修改根用户和普通用户口令？

更改根用户口令的方式和更改普通用户口令的方式相同：先登录到系统，

在命令行方式下输入命令

```
passwd
```

2.12.5 启动应用程序

问题：我从网上下载了一个应用程序，安装过程似乎都一切正常，但在命令行方式下输入程序启动命令的时候，系统提示说找不到该命令。这是什么原因？

如果您试图在命令行方式下启动一个程序的话，最好先试一下给出该命令的完整路径。例如，如果想启动程序 my-executabl，那边就应该输入

```
/usr/local/bin/my-executable
```

假设您从网上下载了 setiathome 的客户端程序，并且将其安装在目录 /home/joe/seti 下，那么启动它的时候应该输入命令 /home/joe/seti/setiathome。必须给出该命令的完整路径才能启动的原因是，在您的环境变量 PATH 中没有给出启动命令 setiathome 所在目录的路径。您可以编辑您主目录下的文件.bash_profile 将 setiathome 的路径添加到环境变量 PATH 中去。步骤如下：

第 1 步 用编辑器打开主目录下的文件.bash_profile

```
        vi ~/.bash_profile
```

您也可以用其他的编辑器打开。

第 2 步 找到环境变量 PATH 所在的那一行，假设显示如下：

```
        PATH=$PATH:$HOME/bin:/usr/local/bin:
```

第 3 步 将 setiathome 所在目录的路径$HOME/seti 追加到后面，结果显示如下：

```
PATH=$PATH:$HOME/bin:/usr/local/bin: $HOME/seti:
```

第 4 步 保持并退出编辑器，执行命令 source .bash_profile 使得刚才的修改立刻生效。

现在您只要直接输入

```
setiathome
```

就可以启动程序了。

2.12.6 快速查看命令

问题：我昨天查看了 man 手册，但我记不清查看的是什么命令的 man 手册了，而且我也没把命令记下来。我怎么样才能找回昨天用过的man命令呢？

您最近使用过的命令都会被存放在一个名为.bash_history 的文件里。不过默认情况下，该文件只保留您最近使用过的 500 条命令。您可以在终端输入命令 history 查看文件.bash_history 中保存的命令，但是结果显得非常快，几乎是一闪而过。查看文件.bash_history 比较好的方法是用命令 less。在终端输入命令

```
less .bash_history
```

文件内容就显示在屏幕上了，按空格键是向下翻页，按[b]键是向上翻页，按[q]是退出。要想找出.bash_history 中所有关于 man 命令的条目，比较快的方法是在终端输入命令

```
history | grep man
```

其中“|”是管道符。关于 grep 的详细用法，可以参考 grep 的手册（man grep）。

2.12.7 history 命令使用小技巧

问题：history 命令有没有其他用法？

如果您只是输入 history 命令，那么屏幕上将显示最近使用过的 500 条命令，而且翻页的速度非常快，一闪而过。但如果您输入 history 20，那么屏幕上只显示您最近使用过的 20 条命令（同理如果输入 50，那么将输出最近使用过的 50 条命令）。

对于 history 还有其他一些使用技巧：

- “感叹号 感叹号”：在终端输入两个感叹号!!，将会执行最近使用过

的一条命令。

• “感叹号 数字”：在终端输入一个感叹号后跟一个数字，将会执行 history 中的指定数字的顺序的命令（例如输入！20，则将会执行第 history 中 20 条命令）。

• “感叹号 字符串”：在终端输入感叹号后跟一个字符串，将会执行最近一个和字符串相匹配的命令（例如输入！ls，则执行最近一次执行的 ls 命令）。

• [向上箭头]和[向下箭头]：在终端中按向上箭头，可以显示上一次执行的命令；如果一直按向上箭头，而越过了要差的命令，可以按向下箭头，往回查看，当想要再次执行的命令出现后，按回车即可执行该命令。

2.12.8 滚动输出 ls 的结果

问题：如果一个目录下的子目录和文件太多，执行一次 ls 后，屏幕向上滚屏太快，我根本看不清显示的结果。怎么样才可以让 ls 的结果不迅速向上滚屏呢？

想要让 ls 显示的结果不滚屏，可以用 ls 命令。例如，要显示/etc 下所有子目录和文件，可以执行命令：

```
ls –al /etc | less
```

按空格键是向下翻页，按[b]键是向上翻页，按[q]是退出。

您还可以用命令：

```
ls –al /etc |   lpr
```

将 ls 的输出结果用打印机打印出来（假设打印机已经配置好）。

2.12.9 访问 windows 分区

问题：我在自己的机器上装了两个系统，一个 windows XP 和一个 GTES10 。我怎么样才能在运行 linux 的时候，访问 windows 的分区呢？

在 linux 下有两种方法可以访问 windows 分区。首先应该确定想要访问的 windows 分区对应的分区号。可以用硬件浏览器查看分区信息，其启动方式为：点击主菜单，选择“系统工具->硬件浏览器”。如图 2-51 所示，在硬件浏览器窗口左边的框内选择硬盘驱动器，右边框内就会显示硬盘分区的信息。

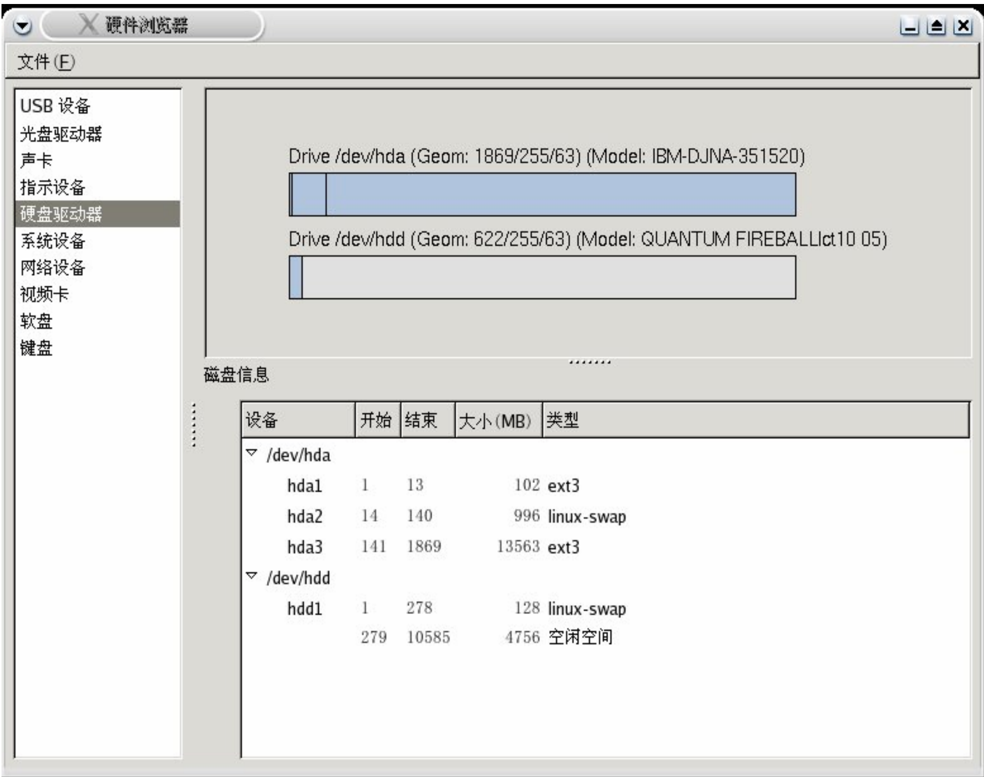


图 2-52 硬件浏览器硬盘分区信息

从硬盘分区信息列表中可以看到，hda1 和 hda5 都是 windows 的分区。下面以访问 hda1 为访问目标，举例说明如何在 linux 下访问 windows 分区。注意：下面的操作需要有根用户权限。

2.12.9.1 临时将 hda1 挂载到系统上

第 1 步 在/mnt 下创建一个用来挂载 windows 分区的目录，假设就创建一个 windows 目录

```
mkdir /mnt/windows
```

第 2 步 将分区 hda1 挂载到目录/mnt/windows 上

```
mount –t vfat /dev/hda1 /mnt/windows
```

第 3 步 访问 windows 分区

```
cd /mnt/windows
```

2.12.9.2 系统启动的时候自动挂载 hda1

第 1 步 在/mnt 下创建一个用来挂载 windows 分区的目录，假设就创建一个 windows 目录

```
mkdir /mnt/windows
```

第 2 步 用编辑器打开文件/etc/fstab（假设用 vi 打开）

```
vi /etc/fstab
```

第 3 步 在文件/etc/fstab 中添加 windows 分区的挂载信息

```
/dev/hda1 /mnt/windows vfat auto,umask=0 0 0
```

第 4 步 存盘退出。

等到下一次启动的时候，hda1 就会自动被挂载到目录/mnt/windows 上了。

2.12.10 安装 RPM 包时输出的出错信息

问题：当我从 CD 上安装一个 RPM 包的时候，屏幕上打印出了出错信息，这是怎么回事？

如果屏幕上打印出来的是类似与“failed to open /var/lib/rpm/packages.rpm”，就说明您的权限还不够，必须是根用户才能安装这个 RPM 包。因为您在

安装软件的时候，必须要拥有全系统范围的修改权限，只有根用户才有这样的权限。

2.12.11 将控制台登录改为图形登录

问题：我怎样才能把控制台登录方式改成图形界面登录呢？

如果您不想在登录后再用命令 startx 来启动图形界面，而且想登录的时候就启动它，那么您只要编辑文件/etc/inittab 就可以了，但必须要根用户权限。其具体步骤如下：

第 1 步 用编辑器打开文件/etc/inittab（假设是用 vi 编辑的）

```
vi /etc/inittab
```

然后您可以看到文件中包含如下信息

```
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
```

第 2 步 将最后一行“id:3:initdefault:”中的 3 改成 5

第 3 步 存盘后退出。

下一次启动的时候，您就就可以以图形方式登录了。

第三章 GTES10 系统管理

3.1 ext3 文件系统

GTES10 默认的文件系统是登记式 ext3 文件系统。

3.1.1 ext3 的特性

一言以蔽之，ext3 文件系统是 ext2 文件系统的增进版本。这些增进提供了以下优越性：

- 可用性

在异常断电或系统崩溃（又称不洁系统关机，unclean system shutdown）发生时，每个在系统上挂载了的 ext2 文件系统必须要使用 e2fsck 程序来检查其一致性。这是一个很费时的过程，特别是在检查包含大量文件的庞大文件卷时，它会大大耽搁引导时间。在这期间，文件卷上的所有数据都不能被访问。

由 ext3 文件系统提供的登记报表方式意味着不洁系统关机后没必要再进行此类文件系统检查。使用 ext3 系统时，一致性检查只在某些罕见的硬件失效（如硬盘驱动器失效）情况下才发生。不洁系统关机后，ext 文件系统的恢复时间不根据文件系统的大小或文件的数量而定，而是根据用于维护一致性的登记日志（journal）的大小而定。根据你的硬件速度，默认的登记日志只需花大约一秒钟来恢复。

- 数据完好性

ext3 文件系统在发送了不洁系统关机时提供更强健的数据完好性。ext3 文件系统允许你选择你的数据接受的保护类型和级别。GTES10 默认配置 ext3 文件卷来保持数据与文件系统状态的高度一致性。

- 速度

尽管 ext3 把数据写入不止一次,它的总处理能力在多数情况小仍比 ext2 系统要高。这是因为 ext3 的登记报表方式优化了硬盘驱动器的头运动。

你可以从三种登记模式中选择来优化速度，但是这么做会在保持数据完好性方面做出一些牺牲。

- 简易转换

你可以轻而易举地不经重新格式化而把 ext2 转换为 ext3 系统，从而获得强健的登记式文件系统的优越性。

如果你执行 GTES10 的完整安装,被分配给系统的 Linux 分区的默认文件系统就是 ext3。如果你从某个使用 ext2 分区的 TDS 版本中升级，安装程序就会允许你把这些分区转换为 ext3 分区，并且不会丢失数据。

以下各节会指导你进行 ext3 分区的创建和微调。

3.1.2 ext3 文件系统

安装后，你有时会有必要创建一个新的 ext3 文件下。譬如，如果你给 TDS 系统添加了一个新的磁盘驱动器，你可能想给这个磁盘驱动器分区，并使用 ext3 文件系统。

创建 ext3 文件系统的步骤如下所列：

- 使用 parted 或 fdisk 来创建分区。
- 使用 mkfs 来把分区格式化为 ext3 文件系统。
- 使用 e2label 给分区标签。
- 创建挂载点。
- 把分区添加到 /etc/fstab 文件中。

3.1.3 转换到 ext3 文件系统

tune2fs 程序能够不改变分区上的已存数据来给现存的 ext2 文件系统添加一个登记报表。如果文件系统在改换期间已被挂载，该登记报表就会被显示为文件系统的根目录中的 .journal 文件。如果文件系统没有被挂载，登记报表就会被隐藏，根本就不会出现在文件系统中。

要把 ext2 文件系统转换成 ext3，登录为根用户后键入：

```
/sbin/tune2fs -j /dev/hdbX
```

在以上命令中，把 /dev/hdb 替换成设备名，把 X 替换成分区号码。

以上命令执行完毕后，请确定把 /etc/fstab 文件中的 ext2 文件系统改成 ext3 文件系统。

如果你在转换你的根文件系统，你将需要使用一个 initrd 映像（或 RAM 磁盘）来引导。要创建它，运行 mkinitrd 程序。

如果改换没有成功，系统仍旧能够引导，只不过文件系统将会被挂载为 ext2 而不是 ext3。

3.1.4 还原到 ext2 文件系统

因为 ext3 相对来说比较新，某些磁盘工具可能还不支持它。例如，你可能需要使用 resize2fs 来缩小某分区，该命令不支持 ext3。在这种情况下，可能会有必要把文件系统暂时还原成 ext2。

要还原分区，你必须首先卸载分区。方法是登录为根用户，然后键入：

```
umount /dev/hdbX
```

在以上命令中，把 /dev/hdb 替换成设备名称，把 X 替换成分区号码。本节以后的示例命令将会使用 hdb1 来代表设备和分区。

下一步，把文件系统类型改回 ext2，以根用户身份键入以下命令：

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

以根用户身份键入以下命令来检查分区的错误：

```
/sbin/e2fsck -y /dev/hdb1
```

然后通过键入以下命令来把分区重新挂载为 ext2 文件系统：

```
mount -t ext2 /dev/hdb1 /mount/point
```

在以上命令中，把 /mount/point 替换成分区的挂载点。

下一步，删除根目录下的 .journal 文件。方法是转换到分区的挂载目录

中，然后键入：

```
rm -f .journal
```

你现在就有一个 ext2 分区了。

如果你永久地把分区改换成 ext2，请记住更新 /etc/fstab 文件。

3.2 访问存取控制列表

文件和目录为它们的所有者、组群、和所有其他系统用户规定了许可权限。但是，这些权限设置也有其局限性。例如：不同的用户无法被配置使用不同的权限。访问存取控制列表（Access Control Lists，ACL）就由此而生。

TDS 内核为 ext3 文件系统和 NFS 导出的文件系统提供 ACL 支持。ACL 在通过 Samba 存取的 ext3 文件系统上也被识别。

除了在内核中的支持外，你还需要 acl 软件包才能实现 ACL。其中包含用来添加、修改、删除、和检索 ACL 信息的工具。

cp 和 mv 命令会复制或转移任何与文件和目录相关的 ACL。

3.2.1 挂载文件系统

在文件或目录中使用 ACL 之前，它们所在的分区必须使用 ACL 支持来挂载。如果它是本地的 ext3 文件系统，它可以使用以下命令来挂载：

```
mount -t ext3 -o acl <device-name> <partition>
```

例如：

```
mount -t ext3 -o acl /dev/hdb3 /work
```

如果分区被列在 /etc/fstab 文件中，该分区的项目就能够包括 acl 选项，如：

```
LABEL=/work      /work       ext3    acl        1 2
```

如果某个 ext3 文件系统是通过 Samba 来存取的，而且其中还启用了

ACL,ACL 就会被识别,这是因为 Samba 已经使用 --with-acl-support 选项被编译了。在存取或挂载 Samba 共享的时候不需要任何特殊标志。

3.2.1.1 NFS

按照默认设置,如果被 NFS 服务器导出的文件系统支持 ACL,并且 NFS 客户能够读取 ACL，ACL 就会被客户系统利用。

在配置服务器的时候，若要禁用 NFS 共享上的 ACL，则在 /etc/exports 文件中包括 no_acl 选项。要在客户上挂载 NFS 共享的时候禁用其中的 ACL，通过命令行或 /etc/fstab 文件使用 no_acl 选项来挂载它。

3.2.2 设置存取 ACL

ACL 有两种：存取 ACL（access ACLs）和默认 ACL（default ACLs)。存取 ACL 是对指定文件或目录的存取控制列表。默认 ACL 只能和目录相关。如果目录中的文件没有存取 ACL,它就会使用该目录的默认 ACL。默认 ACL 是可选的。

ACL 可以按以下条件配置：

- 每用户
- 每组群
- 通过有效权限屏蔽
- 为不属于文件用户组群的用户配置

setfacl 工具为文件和目录设置 ACL。使用 -m 来添加或修改文件或目录的 ACL：

```
setfacl -m <rules> <files>
```

规则(<rules>)必须使用以下格式指定。同一条命令中可以指定多项规则，只要它们是用逗号分开即可。

- u:<uid>:<perms>

为用户设置存取 ACL。用户名或 UID 必须被指定。用户可以是系统上的任何合法用户。

- g:<gid>:<perms>

为组群设置存取 ACL。组群名称或 GID 必须被指定。组群可以是系统上的任何合法组群。

- m:<perms>

设置有效权限屏蔽。该屏蔽是组群所有者和所有用户和组群项目的权限的合集。

- o:<perms>

为文件的组群用户之外的用户设置存取 ACL。

空格被忽略。权限（<perms>）必须是代表读、写、和执行的字符（r、w、x）的组合。

如果某文件或目录已经有了一个 ACL，而 setfacl 命令仍被使用了，额外的规则就会被添加到已存在的 ACL 中，或用来修改已存在的规则。

例如，要给用户 tfox 以读写权限：

```
setfacl -m u:tfox:rw /project/somefile
```

要删除用户、组群或其它人的所有权限，使用 -x 选项，并且不指定任何权限：

```
setfacl -x <rules> <files>
```

例如，删除 UID 为 500 的用户的所有权限：

```
setfacl -x u:500 /project/somefile
```

3.2.3 设置默认的 ACL

要设置默认的 ACL,在规则前面添加 d:,并且指定一个目录而不是文件名。

例如：要把 /share/ 目录的默认 ACL 设置为给不属于用户组群的用户提供读取和执行权（个体文件的存取 ACL 可以超越这个规则）：

```
setfacl -m d:o:rx /share
```

3.2.4 检索 ACL

要判定某个文件或目录的现存 ACL，使用 getfacl 命令：

```
getfacl <filename>
```

它返回的输出和以下相仿：

```
# file: file
# owner: tfox
# group: tfox
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
```

如果指定的是目录，并且它有一个默认的 ACL，默认的 ACL 也会被显示，如：

```
# file: file
# owner: tfox
# group: tfox
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
default:user::rwx
```

3.2.5 给带有 ACL 的文件系统归档

star 工具和 tar 工具相仿。它们都能够被用来生成文件归档。不过，它们的选项有所不同。请参考表 3-1 来获得比较常用的选项列表。要获得所有可用的选项，请参考 star 的说明书页。使用该工具还需要 star 软件包。

选项	描述
-c	创建一个归档文件。
-n	不抽取文件；和 -x 一起用来显示抽取文件会做些什么。
-r	替换归档中的文件。文件被写入归档文件的结尾处，替换带有同样路径和文件名的文件。
-t	显示归档文件的内容。
-u	更新归档文件。如果文件在归档中不存在，或文件比归档中同名的文件更新，它们就会被写入归档的结尾处。该选项只有在归档是文件的时候或者使用一种特殊磁带时才行得通。
-x	从归档中抽取文件。如果和 -U 一起使用，而且归档中的文件比文件系统上的相应文件要老，该文件就不会被抽取。
-help	显示最重要的选项。
-xhelp	显示最不重要的选项。
-/	在从归档中抽取文件时不要剥离文件名中的开头斜线。按照默认设置，这些斜线在文件被抽取时被剥离。
-acl	在创建或抽取时，归档或恢复和文件或目录相关的 ACL。

表 3-1 star 的命令行选项

3.2.6 和旧系统的兼容性

如果 ACL 已经在某个给定文件系统上的某个文件上设置了，该文件系统就会有一个 ext_attr 属性。这个属性可以使用以下命令来查看：

```
tune2fs -l <filesystem-device>
```

得到了 ext_attr 属性的文件系统可以使用较老的内核来挂载，但是那些内核并不强制推行任何被设置了的 ACL。

被包括在版本为 1.22 或更高的 e2fsprogs 软件包中的 e2fsck 工具的几个版本，都能够检查带有 ext_attr 属性的文件系统。较老的版本则拒绝检查它。

3.3 包管理

Turbo Linux 系统中的所有软件均以 RPM 包的形式存在，用户可通过图形化工具或命令行对系统中的软件包进行安装、删除和升级操作。

RPM 包管理器是一个开放的系统，运行在包括 Turbo Linux 在内的大多数 Linux 平台上。

对最终用户来说，软件包的安装、删除和升级都可通过简短的命令完成。RPM 维护系统中所安装软件包的所有信息，因此，用户可通过 RPM 强大的查询选项对系统安装软件包进行查询或校验。

软件包升级时，RPM 会仔细处理用户的配置文件，因此不会出现由于软件升级而导致配置丢失的情况。

对开发者来说，可以通过 RPM 将软件源代码打成包，并以源码包或二进制包的形式提供给最终用户。这些过程由一个包 SPEC 描述文件驱动，SPEC 文件包含了编译该软件包所需的所有信息，如：源代码，补丁以及编译指令等等，当软件有新版本发布时，就能够极大地提高软件包的可维护性。

由于 RPM 将改写系统文件，因此，必须是 root 用户才能进行软件包的安装、删除或升级。

理解 RPM 的设计目标对于更好的使用 RPM 包管理工具是有益的，具体来说，RPM 的设计目标包括如下几个方面：

- 可升级性

使用 RPM 可以升级单个软件包而不需要重新安装整个系统。当基于 RPM 的 Linux 系统发行新版本时，RPM 可以智能化、自动地升级现有的系统。软件包中的配置文件在升级时被保留，因此用户定制的配置信息不会丢失。

- 强大的查询功能

RPM 设计时提供了强大的查询功能。你可以在整个包管理数据库中搜索指定的软件包或文件。你还可以轻易地知道哪个文件属于哪个软件包，软件包来自哪里。每个 RPM 包有一个二进制头，其中包含软件包本身及其内容的信息，包中的文件被压缩存储，这样就允许快速简捷地查询软件包。

- 系统校验

RPM 另一项强大的功能是软件包校验。如果担心可能删除了某软件包中的一个重要文件，只需校验该软件包即可知道是否有这种情况。必要时，可以重装该软件包，修改过的配置文件在重装时会被 RPM 保留。

- 纯净源码

一个重要的设计目标是允许使用所谓“纯净”软件源码，即由软件作者发布的没有打过任何补丁的源码。RPM 将“纯净”源码、所用的补丁、以及完整的编译指令放在一个描述文件中，用来驱动将来的包管理过程。这是一个重要的优点，理由有几个，例如，如果软件有新版本推出，你不必从头开始整个编译过程，因为所有缺省的编译选项，补丁信息，要生成的二进制包中文件的列表等等都包含在描述文件了。

保持源码“纯净”不仅对开发者重要，它也保证了给最终用户提供的软件的质量。

3.3.1 RPM 用法

RPM 有五种最基本的操作：安装、删除、升级、查询和校验。下面将介绍这些操作的一般用法，详细情况可参考: man rpm。

3.3.1.1 安装

假设要安装的软件包名为：foo-1.0-1.i386.rpm，用 root 用户登录到系统，运行以下命令：

```
rpm -ivh foo-1.0-1.i386.rpm
```

如果安装成功，将显示如下信息：

```
Preparing...
########################################### [100%]
   1:foo
########################################### [100%]
```

RPM 从版本 4.1 开始，在安装或升级软件包时会检查软件包的签名。如果签名验证失败，将显示如下错误信息：

```
error: V3 DSA signature: BAD, key ID 0352860f
```

如果仅是一个新的文件头签名，将显示如下错误信息：

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

如果系统中没有相应的密钥来验证该签名，将显示如下警告信息：

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

安装过程比较简单，但也可能出现下面错误：

- 已经安装的包

如果系统中已安装有同样版本的软件包，将显示如下信息：

```
Preparing...
########################################### [100%]
```

```
package foo-1.0-1 is already installed
```

这种情况下，如果仍然要强行安装，可以使用—replacepkgs 选项，此时，RPM 将忽略该错误：

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

该选项在删除了原来安装的 RPM 包中的一些文件，或者想恢复初始时配置文件的情况下有用。

- 冲突的文件

如果要安装的软件包与已安装的软件包包含有相同名字的文件，将显示如下信息：

```
Preparing...
########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

可以使用—replacefiles 选项让 RPM 忽略此错误：

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

- 不能解析的依赖

RPM 包有时会依赖其它的软件包，只有安装了这些被依赖的包，该软件包才能正常运行，如果依赖关系没有解决，将显示如下类似信息：

```
error: Failed dependencies:
        bar.so.2 is needed by foo-1.0-1
    Suggested resolutions:
        bar-2.0.20-3.i386.rpm
```

如果仍然要强行安装，可以使用—nodeps 选项，这将可能导致该软件包不能正常运行，因此不建议这样做。

3.3.1.2 删除

删除软件包和安装一样简单，在提示符下输入如下命令：

```
rpm -e foo
```

如果系统中有其它软件包依赖要删除的软件包，那么将显示如下类似信息：

```
error: Failed dependencies:
        foo is needed by (installed) bar-2.0.20-3.i386.rpm
```

此时也可以用—nodeps 选项强制 RPM 删除该软件包，但这将导致依赖关系被破坏。

3.3.1.3 升级

与安装类似，升级软件包时输入以下命令：

```
rpm -Uvh foo-1.0-1.i386.rpm
```

RPM 将自动删除系统中相应的旧包。实际上也可以使用-U 命令来安装软件包，而不管系统中有无该软件包的以前版本。

如果系统中有软件包升级时需要更新的配置文件，那么将显示如下类似信息：

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

该信息意味着新的配置文件不能前向兼容系统中原有配置文件，原有配置文件被更名保存，新的配置文件安装进去。此时应该马上对比一下新老配置文件的不同，确保系统仍能正常运行。

如果 RPM 认为要升级的软件包比系统中原有的旧，则提示如下类似信息：

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

可以使用—oldpackage 选项强制 RPM 升级。

3.3.1.4 更新

更新与升级类似，命令如下：

```
rpm -Fvh foo-1.0-1.i386.rpm
```

与升级不同的是，如果系统中没有相应的旧包，将不执行安装操作。

3.3.1.5 查询

可以用-q 命令对安装的软件包执行查询操作。如：rpm -q foo 将显示包的名字、版本号、发行号：foo-2.0-1

除了可以指定包的名称，也可以使用以下选项来配合-q 命令执行各项查询操作：

- -a 查询所有已安装的软件包
- -f <文件名> 查询哪个包包含有指定的文件
- -p <包名> 查询指定的软件包

同样，-q 命令也有丰富的选项来指明执行查询操作时将显示什么信息：

- -i 显示包的名称、描述、版本号、发行号、大小、编译时间、安装时间和提供商等信息
- -l 显示包中所有文件的列表
- -s 显示包中所有文件的状态
- -d 显示包中所有的文档文件
- -c 显示包中所有的配置文件

对于显示文件列表的选项，可以附加-v 选项来显示详细信息。

3.3.1.6 校验

RPM 使用-V 命令校验软件包，校验内容包括：大小、MD5 校验和、类型以及文件所属的用户和组等。可以与-V 命令配合使用的校验选项有：

- -f <文件名> 校验指定文件所属的软件包，例如: rpm -Vf /usr/bin/vim

- -a 校验所有已安装的软件包，例如:

```
rpm -Va
```

- -p <包名> 用指定的软件包校验已安装的软件包，例如:

```
rpm -Vp foo-1.0-1.i386.rpm
```

如果校验一切正常，将没有输出，反之则输出不一致结果，格式为:

```
xxxxxxxx   文件名
```

字段 1 由八个字符组成，每个字符指明该文件与 RPM 数据库中一致或不一致的地方，单个点（.）说明没有异常，具体含义如下：

- 5 — 校验和
- S — 文件大小
- L — 符合连接
- T — 文件修改时间
- D — 设备
- U — 用户
- G — 组
- M — 文件模式
- ? — 文件不可读

如果有任何输出显示，请判断是否真的有问题，然后决定删除或重安装异常的软件包，或者通过其它方式解决。

3.3.2 检查包的签名

如果仅想知道 RPM 包是否已损坏或被恶意篡改，可以用下面命令来验证包的 MD5 校验和：

```
rpm -K --nosignature <rpm-file>
```

正常情况下将显示如下信息：

```
<rpm-file>: md5 OK
```

如要看到更详细的消息，可以加 vv 选项，如：

```
rpm -Kvv --nosignature <rpm-file>
```

另一方面，软件包开发者的可信度如何？如果该软件包使用了开发者的 GnuPG 密钥签名，你就会知道开发者的身份是否如他们声称的那样。

GnuPG 工具用于安全通信，而且完全替代了 PGP。你可以用 GnuPG 来验证文档的有效性以及对要发送（接送）的文档加密（解密），同时，GnPG 也能处理 PGP 5.x 的文件。

缺省时系统中已经安装有 GnuPG, 因此，你可以马上用它来验证 RPM 包。但是，首先必须导入 Turbolinux 的公开密钥。

3.3.2.1 导入密钥

在可以检查包的签名前，必须用下面命令导入 Turbolinux 的公开密钥：

```
rpm –import /usr/share/gpg-pubkey/RPM-GPG-KEY
```

下面命令可以显示系统中已安装的公开密钥：

```
rpm -qa gpg-pubkey*
```

3.3.2.2 验证包的签名

导入密钥后，检查 RPM 包的 GnuPG 签名时可运行下面命令：

```
rpm -K <rpm-file>
```

3.3.3 一些示例

用户有时候会误删一些文件，但却不知道到底删了哪些文件，这时可以运行下面命令来检查整个系统：

```
rpm -Va
```

遇到不认识的文件时，可以这样查看它属于哪个包：

```
rpm -qf /usr/bin/ggv
```

把上面两个例子结合起来，下面命令将检查指定文件所属的那个 RPM 包：

```
rpm -Vf /usr/bin/paste
```

要知道一个程序所在 RPM 包的相关文档在哪儿时可运行：

```
rpm -qdf /usr/bin/host
```

查看一个二进制包的详细信息时，执行下面命令：

```
rpm -qpi gcc-3.4.3-9.4.i386.rpm
```

输出结果如下：

```
Name : gcc                Relocations: (not relocatable)
Version : 3.4.3
Vendor: (none)
Release     : 9.4
Build Date: 2005 年 04 月 29 日 星期五 14 时 10 分 13 秒
Install Date: (not installed)
Build Host: dev3-241.dev.cn.tlan
Group       : Development/Languages
Source RPM: gcc-3.4.3-9.4.src.rpm
Size        : 13029656
License: GPL
Signature   : (none)
URL         : http://gcc.gnu.org
Summary     : Various compilers (C, C++, Objective-C, Java, ...)
Description :
The gcc package contains the GNU Compiler Collection version 3.4.
```

```
You'll need this package in order to compile C code.
```

再有，下面命令可以查看包中所有文件列表：

```
rpm -qlp crontabs-1.10-5.noarch.rpm
```

3.3.4 图形化工具

图形化包管理工具提供了图形方式的软件安装、删除和更新功能。

启动该管理工具时，请按以下顺序点击桌面菜单："应用程序 –> 系统设置 –> 添加 / 删除应用程序"，或者在命令行敲入以下命令：system-config-packages。在图形方式下，系统将显示如下界面：



图 3-1 添加或删除软件包主界面

3.3.4.1 安装

包管理工具所有的软件包按功能分成组，每个组由标准软件包和额外软件包组成。标准软件包不能被删除，除非删除整个组。额外软件包的安装可以根据用户的不同要求加以选择。

安装标准软件包时请先选中它所属的组。查看一个组的详细情况时，可点击"细节"连接，这时将显示标准软件包和所有额外软件包列表，如要安装附加软件包，请选中该额外软件包前的小框。例如：



图 3-2 安装软件包界面

上面的选择将安装标准软件包以及除 system-switch-mail-gnome 外的所有额外软件包。关闭子窗口后点击主窗口上的"更新"按钮开始更新当前系统。

3.3.4.2 删除

删除软件包时只需不要取勾选包名前小框的即可，其它操作同安装过程。

因此，在实际包管理时，可以把安装和删除操作合在一个步骤之中。

3.4 网络配置

计算机必须有自己的网络连接才能与其它计算机通讯。操作系统通过识别并配置连接到网络的设备接口（如：以太网、ISDN、调制解调器或令牌环等）来创建一个网络连接。网络管理工具可以用来配置以下几种网络接口：

- 以太网 （Ethernet）
- 综合业务数字网（ISDN）
- 调制解调器（modem）
- xDSL
- 令牌环（token ring）
- 无线设备（wireless devices）

也可以用来配置 IPsec 连接、管理 DNS 设置和/etc/hosts 文件。你必须有 root 权限才能使用网络管理工具。启动时，请按以下顺序点击桌面菜单："应用程序 —> 系统设置 —> 更多系统设置 —> 网络"，或者在命令行敲入以下命令：system-config-network。在图形方式下，系统将显示如下界面：

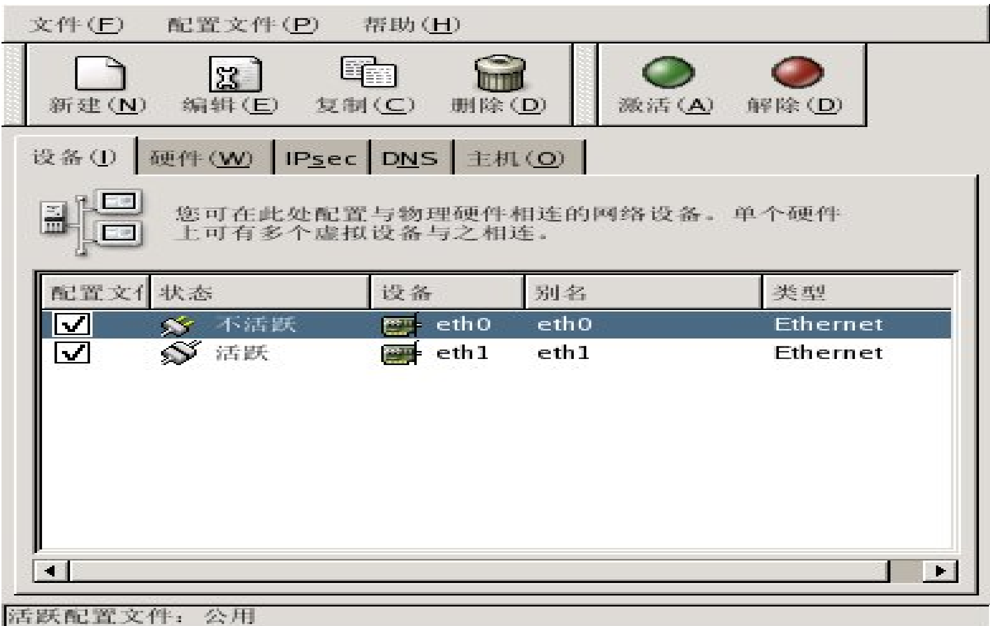


图 3-3 网络配置界面

3.4.1 概览

配置网络连接的一般步骤是：

- 添加一个关连到物理设备的网络设备名。
- 如果硬件列表中没有此物理设备，则添加到硬件列表。
- 配置主机名和 DNS 设置。
- 配置其它不能通过 DNS 查询的主机名。

下面详细介绍配置上述每种网络连接类型的具体步骤。

3.4.2 建立以太网连接

在建立以太网连接前，必须准备好网络接口卡（网卡），网线，以及准备

接入的网络。不同的网络有不同的传输速率，请确保网卡兼容要接入的网络。

请按照以下步骤添加以太网连接：

- 点击“设备”标签
- 点击工具条上的“新建”按钮
- 从设备类型列表中选择“以太网连接”，然后点击“前进”按钮
- 如果网卡已经加入了硬件列表，请选中它，否则选择“其它以太网卡”
- 如果选择了“其它以太网卡”，请在下一个“选择以太网适配器”窗口中配置以太网卡的制造商和类型，并设置设备名，如：eth0, eth1 等。点击“前进”按钮后将出现下面“配置网络设置”窗口：

图 3-4 配置网络设置窗口

- 选择 DHCP 自动获取 IP 地址，或为主机设置静态 IP 地址，然后点击“前进”按钮

- 点击“应用”按钮后可看到新设备已经添加到了设备列表：

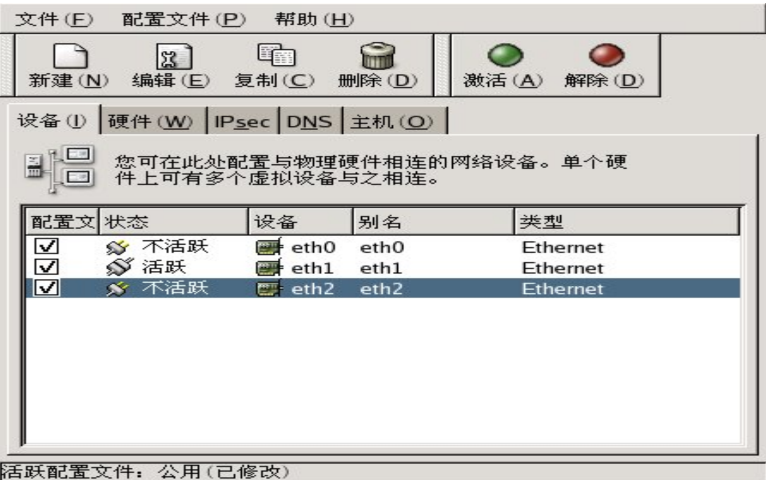


图 3-5 配置网络设置－选择设备

保存配置信息请点击菜单：“文件 —> 保存”

新设备加入后并不自动激活，如要激活请点击“激活”按钮。此外，也可以点击工具条上的“编辑”按钮来配置设备的各项属性。

3.4.3 建立 ISDN 连接

ISDN 连接是一种用 ISDN 调制解调器通过一条特殊的电话线建立的网络连接。

请按照以下步骤添加 ISDN 连接：

- 点击“设备”标签
- 点击工具条上的“新建”按钮
- 从设备类型列表中选择“ISDN 连接”，然后点击“前进”按钮

- 在“选择 ISDN 适配器”窗口中配置适配器所需资源以及 D 频道协议，如下图：



图 3-6 选择 ISDN 窗口

然后点击“前进”按钮

- 配置提供商信息。点击“前进”按钮
- 在“IP 设置”窗口中配置封装模式和 IP 地址获取方式，然后点击“前进”



图 3-7 IP 设置窗口

按钮。

- 点击“应用”按钮将新设备添加到设备列表

3.4.4 建立调制解调器连接

调制解调器可以用来通过一条普通电话线建立因特网连接。建立调制解调器连接时需要 ISP 拨号帐号。

请按照以下步骤添加调制解调器连接：

- 点击“设备”标签
- 点击工具条上的“新建”按钮
- 从设备类型列表中选择“调制解调器连接”，然后点击“前进”按钮
- 如果硬件列表中已经配置有调制解调器，网络管理工具将使用该调制解调器建立网络连接，否则它将试图检测系统中是否有调制解调器，当检测到调制解调器时，将出现如下配置窗口：

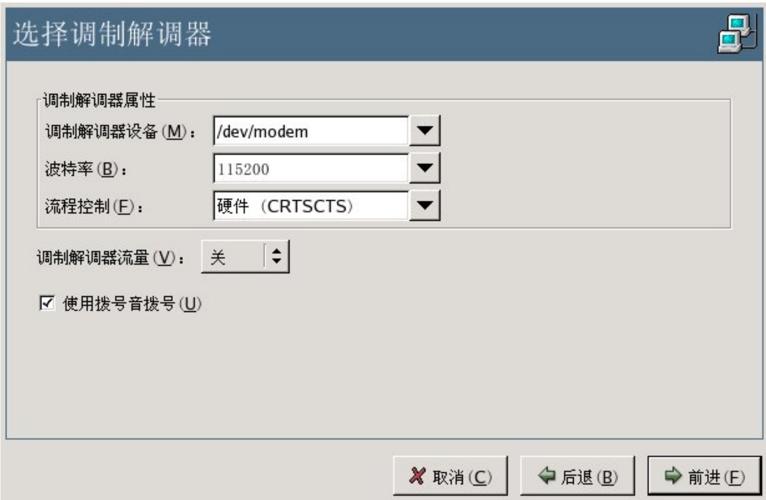


图 3-8 选择调制解调器窗口

- 在上面窗口中配置完调制解调器的设备名、波特率以及流程控制属性等后点击“前进”按钮
- 配置提供商信息。点击“前进”按钮
- 在“IP 设置”窗口中配置封装模式和 IP 地址获取方式，然后点击“前进”按钮
- 点击“应用”按钮将新设备添加到设备列表

3.4.5 建立 xDSL 连接

DSL 是数字用户环路（Digital Subscriber Loop）的英文缩写。目前有几种不同类型的 DSL，如：ADSL，IDSL 和 SDSL 等。网络管理工具用 xDSL 代指所有的 DSL 类型。

有些 DSL 提供商要求配置系统从以太网通过 DHCP 动态获取 IP 地址，有些提供商需要在以太网上配置 PPPoE，具体是何种方式请咨询 DSL 提供商。

请按照以下步骤添加 xDSL 连接：

- 点击“设备”标签
- 点击工具条上的“新建”按钮
- 从设备类型列表中选择“xDSL 连接”，然后点击“前进”按钮

图 3-9 配置 DSL 连接窗口

- 从下拉菜单中选择以太网设备，输入提供商名称、登录名，口令。如果有 T-Online 帐号则不需要输入 登录名和口令，直接点击“T-Online 帐号设置”按钮进行相应设置。配置完毕点击“前进”按钮。
- 点击“应用”按钮将新设备添加到设备列表

3.4.6 建立令牌环连接

请按照以下步骤添加令牌环连接：

- 点击“设备”标签
- 点击工具条上的“新建”按钮

- 从设备类型列表中选择“令牌环连接”，然后点击“前进”按钮
- 如果令牌环卡已经加入了硬件列表，请选中它，否则选择“其它令牌环卡”
- 如果选择“其它令牌环卡”，将显示如下配置窗口：

图 3-10 选择令牌环适配器窗口

选择令牌环适配器的类型，配置设备名（如：tr0, tr1, ...）以及系统资源，然后点击“前进”按钮

- 在配置网络设置窗口，选择 DHCP 自动获取 IP 地址，或为主机设置静态 IP 地址，然后点击“前进”按钮
- 点击“应用”按钮将新设备添加到设备列表

3.4.7 建立无线连接

- 点击“设备”标签
- 点击工具条上的“新建”按钮

- 从设备类型列表中选择“无线连接”，然后点击“前进”按钮
- 如果无线卡已经加入了硬件列表，请选中它，否则选择“其它无线卡”
- 如果选择“其它无线卡”，将显示无线网卡配置窗口，配置无线设备完后点击“前进”按钮
- 在配置网络设置窗口，选择 DHCP 自动获取 IP 地址，或为主机设置静态 IP 地址，然后点击“前进”按钮
- 点击“应用”按钮将新设备添加到设备列表

3.4.8 管理 DNS 设置

“DNS”标签用来配置系统的主机名、域、名字服务器和搜索路径信息。名字服务器用来查询网络上的其它计算机。如果 DNS 服务名字通过 DHCP 或 PPPoE 自动获得，或是由 ISP 提供，则不需要输入名字服务器地址。如果主机名由 DHCP 或 PPPoE 动态提供，则不需要输入主机名。

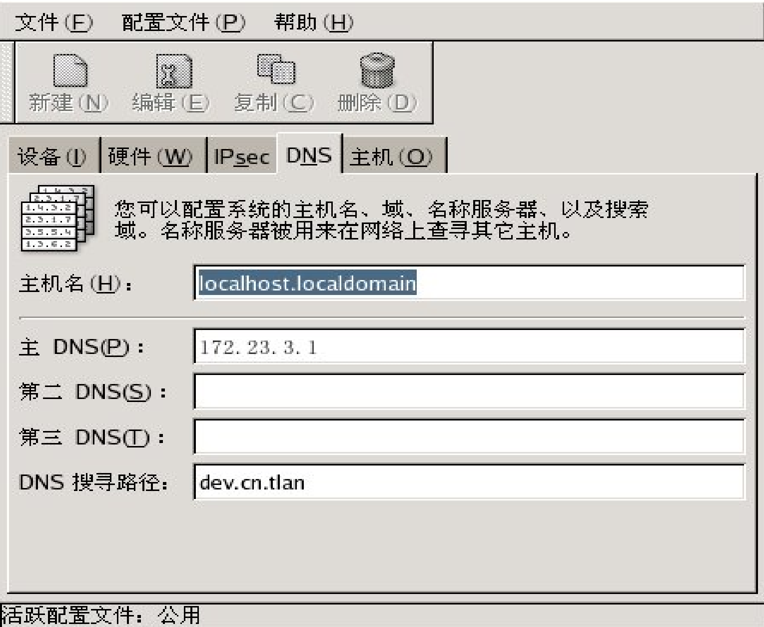


图 3-11 配置 DNS 窗口

3.4.9 管理主机设置

“主机”标签用来从/etc/hosts 文件中添加，编辑或删除主机信息。/etc/hosts 文件是 IP 地址和主机名字的映射表。缺省情况下，系统解析主机的 IP 地址或从 IP 地址解析主机时会首先查询/etc/hosts 文件。

要添加新的对应表，请点击“新建”按钮，然后输入所要求的信息。

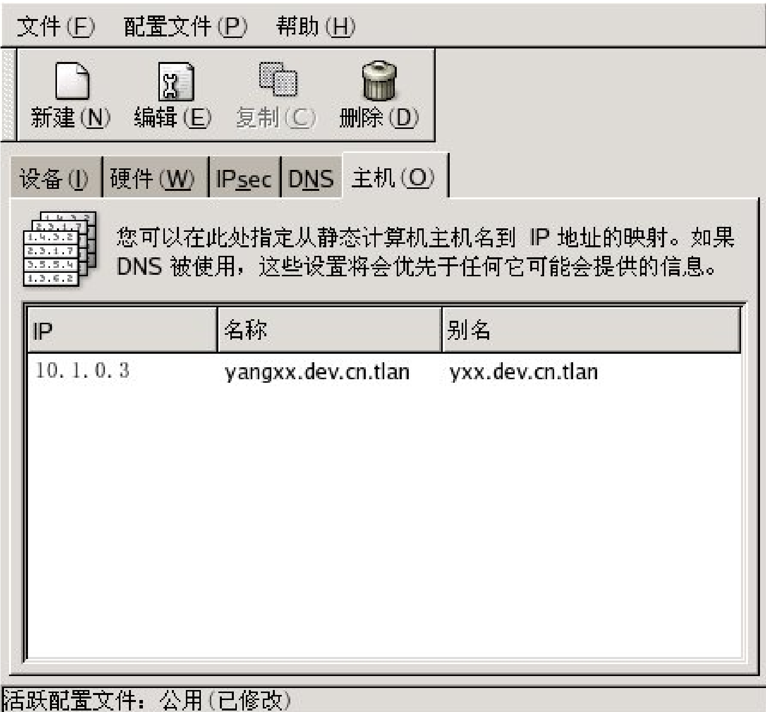


图 3-12 主机设置窗口

3.4.10 设备别名

设备别名是关联到物理硬件的一种虚拟设备，但可以有自己独立的 IP 地址，一般情况下，设备别名用物理设备名跟一个冒号以及一个数字组成，

如：eth0:1。当系统只有一个网卡而需要多个 IP 地址时，就可以使用设备别名。

可以按如下的方式创建设备别名：

点击“新建”按钮，选择网络接口类型（如以太网），选中一个有静态 IP 地址的以太网卡（DHCP 时不支持设备别名），在网络配置时设置静态 IP 地址，此时将创建一个新的别名。

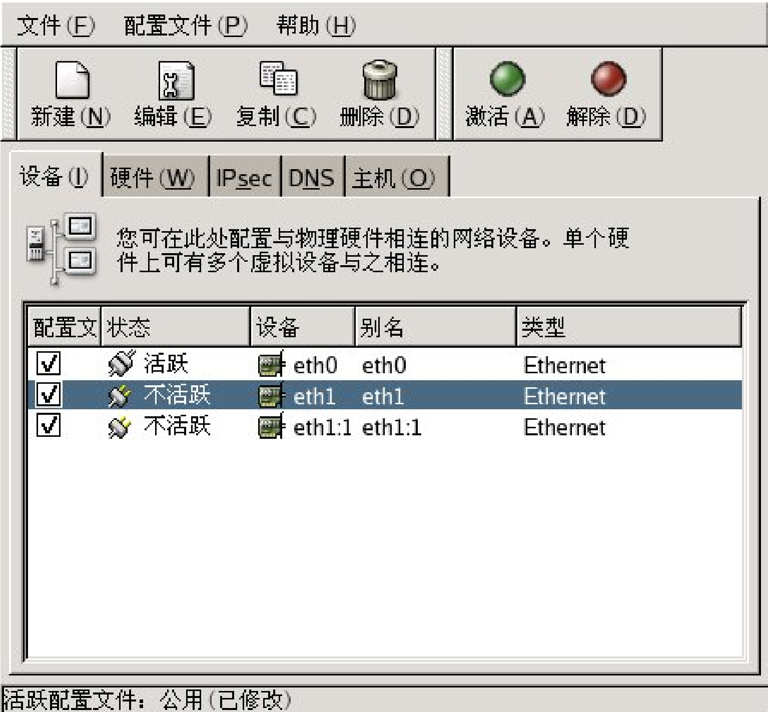


图 3-13 设备别名配置

3.4.11 建立 IPsec 连接

IPsec 是 Internet Protocol Security 的缩写，它是一种虚拟专用网解决方案。IPsec 可以在两个系统或网络间建立一条加密的信道，从而保证数据通讯的安全。

3.4.11.1 主机到主机 IPsec 连接

主机到主机的 IPsec 连接是指在两台同时运行着 IPsec 并有公共密钥的主机间建立一条 IPsec 连接。当 IPsec 连接激活时，两台主机间的通讯将被加密。

请按照以下步骤添加 IPsec 连接：

- 点击“IPsec”标签
- 点击工具条上的“新建”按钮
- 然后点击“前进”按钮配置主机到主机 IPsec 连接
- 为 IPsec 连接选择一个别名， 如：ipsec0。选择该连接是否自动启动
- 选择连接类型：主机到主机加密
- 选择加密类型，如选择固定密钥手工加密，则需指明加密密钥。如选择自动加密模式，则必须运行 racoon 服务管理密钥
- 指定对方 IP 地址
- 点击“应用”按钮并保存设置

3.4.11.2 网络到网络 IPsec 连接

网络到网络 IPsec 连接是指在两台 IPsec 路由器间建立 IPsec 连接。

请按照以下步骤添加 IPsec 连接：

- 点击“IPsec”标签
- 点击工具条上的“新建”按钮
- 然后点击“前进”按钮配置网络到网络 IPsec 连接
- 为 IPsec 连接选择一个别名， 如：ipsec0。选择该连接是否自动启动
- 选择连接类型：网络到网络加密
- 选择加密类型，如选择固定密钥手工加密，则需指明加密密钥。如选择自动加密模式，则必须运行 racoon 服务管理密钥

- 指定本地网络地址，网络掩码和网关
- 指定远程网络地址，网络掩码，子网掩码和网关
- 点击“应用”按钮并保存设置

3.4.11.3 启动和停止 IPsec 连接

如果 IPsec 连接没有配置成系统引导时自动启动，可以通过命令行启动或停止 IPsec 连接。例如：

- 启动别名为 ipsec0 的 IPsec 连接时执行：

```
/sbin/ifup ipsec0
```

- 停止别名为 ipsec0 的 IPsec 连接时执行：

```
/sbin/ifdown ipsec0
```

3.4.12 保存和恢复网络配置

在命令行方式下，可以将网络配置信息保存在文件中。例如，下面命令将把网络配置信息保存在文件/tmp/network-config 中：

```
system-config-network-cmd -e > /tmp/network-config
```

反之，从/tmp/network-config 文件中恢复网络配置信息时可运行：

```
system-config-network-cmd -i -c -f /tmp/network-config
```

3.5 防火墙配置基础

计算机防火墙可以防止病毒的扩散以及未经授权的计算机访问。防火墙位于计算机和网络之间，通过规则设置来控制网络上的哪些远程计算机可以访问本地计算机上的哪些服务。配置正确的防火墙可以极大提高计算机的安全性。因此，如果计算机要连入因特网，建议启用防火墙。

3.5.1 安全级别配置工具

安全级别配置工具用来配置系统安全性的相关设置。

启动该管理工具时，请按以下顺序点击桌面菜单："应用程序 —> 系统设置 —> 安全级别"，或者在命令行敲入以下命令：system-config-securitylevel。在图形方式下，系统将显示如下界面：



图 3-14 安全级别配置

安全级别配置工具只能配置简单的防火墙，若需要更复杂的规则控制，请参考 iptables 帮助。

3.5.1.1 启用和禁用防火墙

- 禁用防火墙：不做任何安全检查，允许任何网络用户访问计算机上的服务。如果不是可信任网络，不建议使用此选项。
- 启用防火墙：拒绝所有的 incoming 连接。如果计算机不用作服务器，这是一个安全的选择。

3.5.1.2 信任的服务

如果想允许特定的服务可以通过防火墙，请选择相应的选项：

- WWW (HTTP)

HTTP 协议用来提供 WWW 服务，如果该计算机用作 WWW 服务器，请选择此选项。

- FTP

FTP 协议用来提供文件传输服务，如果该计算机用作 FTP 服务器，请选择此选项。

- SSH

SSH 是包括远程登录，命令执行和文件拷贝在内的一系列工具，允许 ssh 访问时请选择此选项。

- Telnet

Telnet 是远程登录协议，由于 Telnet 采用不加密通讯，因此不建议打开此选项。

- Mail(SMTP)

如果该计算机用作邮件服务器，请选择此选项。

3.5.1.3 信任的设备

选择任何一个“信任的设备”将使该设备不受防火墙规则的控制，这也意味着允许所有来自该网络设备的数据通讯。例如，本地网络上的计算机通

过 PPP 拨号连接到了互联网上，如果选择“eth0”作为信任的设备 ，那么将允许所有来自本地网络的数据通讯。但是通过 ppp0 接口的通讯仍受防火墙规则的限制。

建议你不要把连接到公共网络（如因特网）上的设备设为“信任的设备”。

3.5.1.4 其它端口

安全级别配置工具可以定制其它 IP 端口列表以便从这些端口进出的数据可以通过防火墙。例如，允许 NFS，IRC，IPP 通过防火墙时可作如下设置：

```
2049:tcp,194:tcp,631:tcp
```

3.5.1.5 保存设置

点击“确定”按钮保存当前的设置，设置信息将被存在/etc/sysconfig/iptables 和/etc/sysconfig/system-config-securitylevel 文件中，下次安全级别配置工具启动时将会读取这些文件，因此不建议手工修改它们。

3.5.2 启动 iptables 服务

只有 iptables 服务启动后上面所述的防火墙规则才能起作用，可用下面命令手工启动 iptables 服务：

```
/sbin/service iptables restart
```

如要在系统引导之时启动 iptables 服务，请执行下面命令：

```
/sbin/chkconfig --level 345 iptables on
```

Turbo Linux 发行版现已不包含 ipchains 服务，如果 ipchains 已经手工安装，请确保 ipchains 服务不与 iptables 服务同时启动，停止 ipchains 服务，请执行下面命令：

```
/sbin/service ipchains stop
```

停用 ipchains 服务，请执行下面命令：

```
/sbin/chkconfig

          --level 345 ipchains off
```

3.6 服务访问控制

系统安全的维护对计算机来说是极其重要的，一个重要的安全措施便是控制对计算机服务的访问。所有服务仅仅当它们是必不可少时才应该启动。对于不必要的服务都应该禁止，这可将把可能的漏洞攻击降到最低。

服务访问控制可有多种方法，具体采用什么方法决定于服务的类型、计算机的配置情况以及管理员的水平。

拒绝远程计算机访问某一服务的最简便方法是将其关闭。不论是由 xinetd（我们会在本节后面详细讨论）管理的服务，还是在 /etc/rc.d 中的服务，都可以用以下三种应用程序将其启动或停止：

- 服务配置工具 — 图形化应用程序。它在窗口中显示每项服务的描述，以及每项服务是否在引导时启动（运行级别 3、4、5），并允许你启动、停止或重新启动每项服务。
- ntsysv — 基于文本的程序。允许为每个运行级别配置系统引导时启动的服务。ntsysv 不能用来启动、停止或重新启动不属于 xinetd 管理的服务。
- chkconfig — 命令行工具。允许为每个运行级别配置系统引导时要启动的服务。但不能用来启动、停止或重新启动不属于 xinetd 管理的服务。

另外一种服务访问控制的方法是用 iptables 配置防火墙，对于新手来说 iptables 可能比较复杂，它更适合有经验的系统管理员。但是，iptables 的优点在于它的灵活性，更详细的信息请参考 iptables 帮助。

作为一般性的选择，可以运行安全级别配置工具来配置系统，它可满足大多数常规的应用。

3.6.1 运行级别

在配置服务访问控制之前，必须理解 Linux 系统的运行级别。运行级别是

一种状态，或模式（mode），它由列在 /etc/rc.d/rc<x>.d 目录中的服务来定义，其中 <x> 是运行级别的数字表示。

存在下列运行级别：

- 0 — 停止
- 1 — 单用户模式
- 2 — 没有使用（由用户定义）
- 3 — 有网络的多用户模式
- 4 — 没有使用（由用户定义）
- 5 — 有网络的多用户模式，并且支持 X 窗口
- 6 — 重新引导

如果使用文本方式登录，运行级别是 3。如果图形登录，运行级别为 5。

可以通过修改 /etc/inittab 文件来改变默认的运行级别，例如：

```
id:5:initdefault:
```

将上面的数字改为期望的运行级别，所做改变在系统重新引导时才生效。

如果要立即改变运行级别，请使用 telinit 命令，后跟运行级别数字。只有 root 用户才能使用该命令。telinit 命令只会改变当前运行级别而不会修改 inittab 文件。

3.6.2 TCP 包裹程序

许多 UNIX 系统管理员比较熟悉 TCP 包裹程序。xinetd 管理的服务以及其它任何内建支持 libwrap 的服务都能够通过 TCP 包裹程序来进行访问控制。TCP 包裹程序通过配置/etc/hosts.allow 和 /etc/hosts.deny 文件来控制哪些网络上的其它计算机可以访问哪些服务。其中，hosts.allow 是允许访问规则列表，hosts.deny 是拒绝访问规则列表，具体格式请参考：man 5 hosts_access。

3.6.2.1 xinetd

为了更好的保障计算机安全，xinetd 已经替代了过去的 xinetd 服务程序。xinetd 提供了访问控制功能、日志记录功能，同时也可以支持其它非标准服务。xinetd 可以针对每一台计算机，每一时段作访问控制，限制 incoming 连接的频率，限制连接的负载。

启动时 xinetd 对管理的所有服务端口进行监听，当服务请求到达时，xinetd 启动相应的服务程序进行处理。

启用或禁止 xinetd 服务时请修改/etc/xinetd.d 目录中的相应文件。如果 disable 属性设置为 yes，该服务将被禁用，设置为 no 时，该服务将被启用。当然也可通过服务配置工具，ntsysv, 或者 chkconfig 对此进行修改。

3.6.3 服务配置工具

服务配置工具是一个用来配置/etc/rc.d/init.d 中 SysV 服务的图形化配置程序，启动该管理工具时，请按以下顺序点击桌面菜单：“应用程序 —> 系统设置 —>服务配置 —>服务，或者在命令行敲入以下命令：system-config-services。在图形方式下，系统将显示如下界面：

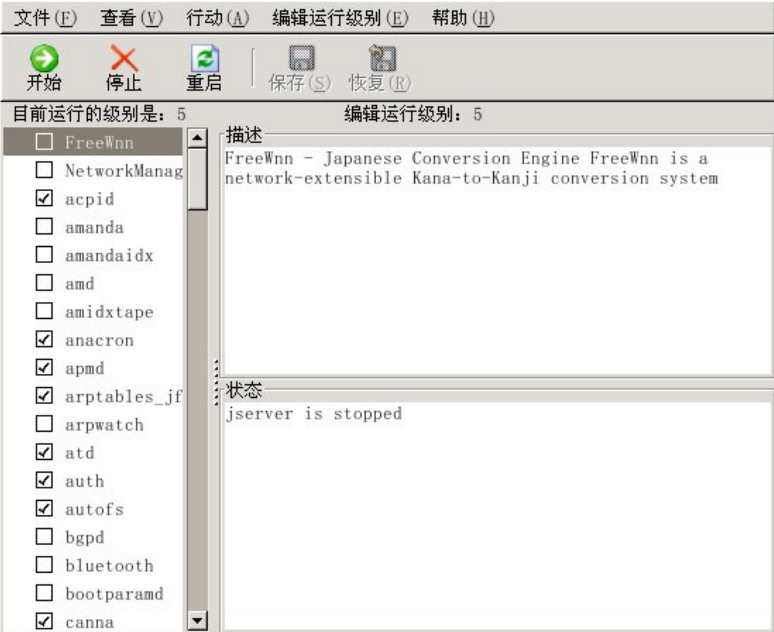


图 3-15 服务配置工具

服务配置工具显示当前的运行级别和编辑中的运行级别。如要改变编辑运行级别，请从“编辑运行级别”菜单中选取。

服务配置工具在左边窗口同时显示/etc/rc.d/init.d和xinetd管理的服务列表，可单击服务名字来查看服务描述和状态信息。

如要启动，停止或重新启动服务，请点击工具条上的相应按钮。

3.6.4 ntsysv

ntsysv 提供了一种启动或停止服务的简便方法，也可以用来配置系统运行级别，缺省时仅配置当前运行级别中的服务，加—level 选项时可指明所配置的运行级别，例如：

```
ntsysv --level 345
```

3.6.5 chkconfig

chkconfig 命令也可以用来启用或禁止服务。运行 chkconfig --list 命令可以看到当前系统服务列表，以及它们在不同运行级别中的状态。列表后半部分是 xinetd 管理服务。

例如：命令 chkconfig --list anacron 返回下列输出：

```
anacron   0:关闭   1:关闭   2:启用   3:启用   4:启用   5:启用   6:关闭
```

又如，命令 chkconfig --list finger 返回下列输出：

```
finger       关闭
```

chkconfig 还能用来设置某一服务在某一指定的运行级别内被启动或禁止。譬如，要在运行级别 3、4、5 中禁止 nscd 服务，可使用下面的命令：

```
chkconfig --level 345 nscd off
```

3.7 OpenSSH

OpenSSH 是 SSH （Secure SHell） 协议的免费开源实现。它用安全、加密的网络连接工具代替了 telnet、ftp、 rlogin、rsh 和 rcp 工具。OpenSSH 支持 SSH 协议的版本 1.3、1.5、和 2。自从 OpenSSH 的版本 2.9 以来，默认的协议是版本 2，该协议默认使用 RSA 钥匙。

3.7.1 为什么使用 SSH

使用 OpenSSH 工具将会增进你的系统安全性。 所有使用 OpenSSH 工具的通讯，包括口令，都会被加密。 telnet 和 ftp 使用纯文本口令，并被明文发送。这些信息可能会被截取，口令可能会被检索，然后未经授权的人员可能会使用截取的口令登录进你的系统而对你的系统造成危害。你应该尽可能地使用 OpenSSH 的工具集合来避免这些安全问题。

另一个使用 OpenSSH 的原因是，它自动把 DISPLAY 变量转发给客户机器。换一句话说，如果你在本地机器上运行 X 窗口系统，并且使用 ssh 命令登录到了远程机器上，当你在远程机器上执行一个需要 X 的程序时，它会显示在你的本地机器上。如果你偏爱图形化系统管理工具，却不能够总是亲身访问该服务器，这就会为你的工作大开方便之门。

3.7.2 配置 OpenSSH 服务器

要运行 OpenSSH 服务器，你必须首先确定你安装了正确的 RPM 软件包。openssh-server 软件包是必不可少的，并且它依赖于 openssh 软件包的安装与否。

OpenSSH 守护进程使用 /etc/ssh/sshd_config 配置文件。默认配置文件在多数情况下应该足以胜任。如果你想使用没有被默认的 sshd_config 文件提供的方式来配置守护进程，请阅读 sshd 的说明书（man）页来获取能够在配置文件中定义的关键字列表。

要启动 OpenSSH 服务，使用 /sbin/service sshd start 命令。要停止

OpenSSH 服务器，使用 /sbin/service sshd stop 命令。

如果你重新安装了，任何在它被重装前使用 OpenSSH 工具连接到这个系统上的客户在它被重装后将会看到下列消息：

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle
attack)!

It is also possible that the RSA host key has just been changed.
```

重装后的系统会为自己创建一组新的身份标识钥匙;因此客户会看到 RSA 主机钥匙改变的警告。如果你想保存系统原有的主机钥匙，备份 /etc/ssh/ssh_host*key* 文件，然后在系统重装后恢复它。该过程会保留系统的身份。当客户机在该系统重装后试图连接它，它们就不会看到以上的警告信息。

3.7.3 配置 OpenSSH 客户

要从客户机连接到 OpenSSH 服务器上，你必须在客户机器上装有 openssh-clients 和 openssh 软件包。

3.7.3.1 使用 ssh 命令

ssh 命令是 rlogin、rsh 和 telnet 命令的安全替换。它允许你在远程机器上登录并在其上执行命令。

使用 ssh 来登录到远程机器和使用 telnet 相似。要登录到一个叫做 penguin.example.net 的远程机器，在 shell 提示下键入下面的命令：

```
ssh penguin.example.net
```

第一次使用 ssh 在远程机器上登录时，你会看到和下面相仿的消息：

```
The authenticity of host 'penguin.example.net' can't be establ\
ished.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:\
e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

键入 yes 来继续。这会把该服务器添加到你的已知主机的列表中，如下面的消息所示：

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list
of known hosts.
```

下一步，你会看到向你询问远程主机口令的提示。在输入口令后，你就会在远程主机的 shell 提示下了。如果你没有指定用户名，你在本地客户机器上登录用的用户名就会被传递给远程机器。如果你想指定不同的用户名，使用下面的命令：

```
ssh username@penguin.example.net
```

你还可以使用 ssh -l username penguin.example.net。

ssh 命令可以用来在远程机器上不经 shell 提示登录而执行命令。它的语法格式是： ssh hostname command。譬如，如果你想在远程主机 penguin.example.net 上执行 ls /usr/share/doc 命令，在 shell 提示下键入下面的命令：

```
ssh penguin.example.net ls /usr/share/doc
```

在你输入了正确的口令之后， /usr/share/doc 这个远程目录中的内容就会被显示，然后你就会被返回到你的本地 shell 提示下。

3.7.3.2 使用 scp 命令

scp 命令可以用来通过安全、加密的连接在机器间传输文件。它与 rcp 相似。

把本地文件传输给远程系统的一般语法是：

```
scp localfile username@tohostname:/newfilename
```

localfile 指定源文件，username@tohostname:/newfilename 指定目标文件。

要把本地文件 shadowman 传送到你在 penguin.example.net 上的账号内，在 shell 提示下键入（把 username 替换成你的用户名）：

```
scp shadowman username@penguin.example.net:/home/username
```

这会把本地文件 shadowman 传输给 penguin.example.net 上的 /home/username/shadowman 文件。

把远程文件传输给本地系统的一般语法是：

```
scp username@tohostname:/remotefile /newlocalfile
```

remotefile 指定源文件，newlocalfile 指定目标文件。

源文件可以由多个文件组成。譬如，要把目录 /downloads 的内容传输到远程机器 penguin.example.net 上现存的 uploads 目录，在 shell 提示下键入下列命令：

```
scp /downloads/* username@penguin.example.net:/uploads/
```

3.7.3.3 使用 sftp 命令

sftp 工具可以用来打开一次安全互动的 FTP 会话。它与 ftp 相似，只不过，它使用安全、加密的连接。它的一般语法是：sftp username@hostname.com。一旦通过验证，你可以使用一组和使用 FTP 相似的命令。sftp 工具只在 OpenSSH 版本 2.5.0p1 以上才有。

3.7.3.4 生成钥匙对

如果你不想每次使用 ssh、scp 或 sftp 时都要输入口令来连接远程机器，你可以生成一对授权钥匙。

钥匙必须为每个用户生成。要为某用户生成钥匙，用想连接到远程机器的用户身份来遵循下面的步骤。如果你用根用户的身份完成了下列步骤，就

只有根用户才能使用这对钥匙。

从 OpenSSH 版本 3.0 开始，~/.ssh/authorized_keys2、~/.ssh/known_hosts2 和 /etc/ssh_known_hosts2 就会过时。SSH 协议 1 和 2 共享 ~/.ssh/authorized_keys、~/.ssh/known_hosts 和 /etc/ssh/ssh_known_hosts 文件。

GTES10 默认使用 SSH 协议 2 和 RSA 钥匙。

3.7.3.4.1 为版本 2 生成 RSA 钥匙对

使用下列步骤来为 SSH 协议的版本 2 生成 RSA 钥匙对。从 OpenSSH 2.9 开始，它已成为默认设置。

要生成 RSA 钥匙对与协议的版本 2 合作，在 shell 提示下键入下列命令：

```
ssh-keygen -t rsa
```

接受 ~/.ssh/id_rsa 的默认位置。输入一个与你的帐号口令不同的口令句，再输入一次来确认。

公钥被写入 ~/.ssh/id_rsa.pub。密钥被写入 ~/.ssh/id_rsa。决不能把密钥出示给任何人。

使用以下命令改变你的 .ssh 目录的许可权限：

```
chmod 755 ~/.ssh
```

把 ~/.ssh/id_rsa.pub 的内容复制到你想连接的机器上的 ~/.ssh/authorized_keys 文件中。如果 ~/.ssh/authorized_keys 不存在，你可以把 ~/.ssh/id_rsa.pub 文件复制到那个机器上的 ~/.ssh/authorized_keys 文件中。

使用以下命令改变你的 authorized_keys 文件的许可权限：

```
chmod 644 ~/.ssh/authorized_keys
```

3.7.3.4.2 为版本 2 生成 DSA 钥匙对

使用下面的步骤来为 SSH 协议的版本 2 生成 DSA 钥匙对。

要生成用于协议的版本 2 的 DSA 钥匙对，在 shell 提示下键入下面的命令：

```
ssh-keygen -t dsa
```

接受 ~/.ssh/id_dsa 的默认位置。输入一个与你的帐号口令不同的口令句，再输入一次来确认。

公钥被写入 ~/.ssh/id_dsa.pub。密钥被写入 ~/.ssh/id_dsa。决不能把密钥出示给任何人，这一点很重要。

使用以下命令改变你的 .ssh 目录的许可权限：

```
chmod 755 ~/.ssh
```

把 ~/.ssh/id_dsa.pub 的内容复制到你想连接的机器中的 ~/.ssh/authorized_keys 文件中。如果文件 ~/.ssh/authorized_keys 不存在，你可以把 ~/.ssh/id_dsa.pub 文件复制到那个机器上的 ~/.ssh/authorized_keys 文件中。

使用以下命令改变你的 authorized_keys 文件的许可权限：

```
chmod 644 ~/.ssh/authorized_keys
```

3.7.3.4.3 为版本 1.3 和 1.5 生成 DSA 钥匙对

使用下面的步骤来生成用于 SSH 协议版本 1 的 RSA 钥匙对。如果你只在使用 DSA 的系统间连接，则不需要 RSA 版本 1.3 或 RSA 版本 1.5 钥匙对。

要生成 RSA （版本 1.3 和 1.5 协议）钥匙对，在 shell 提示下键入下列命令：

```
ssh-keygen -t rsa1
```

接受默认的位置 （~/.ssh/identity）。输入和你的帐号口令不同的口令句。再输入一次来确认。

公钥被写入 ~/.ssh/identity.pub。密钥被写入 ~/.ssh/identity。不要把你的密

钥出示给任何人。

使用 chmod 755 ~/.ssh 和 chmod 644 ~/.ssh/identity.pub 命令改变你的 .ssh 目录和密钥的许可权限。

把 ~/.ssh/identity.pub 的内容复制到你想连接的机器中的 ~/.ssh/authorized_keys 文件中。如果文件 ~/.ssh/authorized_keys 不存在，你可以把 ~/.ssh/identity.pub 文件复制到远程机器上的 ~/.ssh/authorized_keys 文件中。

3.8 网络文件系统—NFS

网络文件系统（NFS）是一种在网络上的机器间共享文件的方法，文件就如同位于客户的本地硬盘驱动器上一样。Turbolinux DataServer 既可以是 NFS 服务器也可以是 NFS 客户，这意味着它可以把文件系统导出给其它系统，也可以挂载从其它机器上导入的文件系统。

3.8.1 为什么使用 NFS

NFS 对于在同一网络上的多个用户间共享目录很有用途。譬如，一组致力于同一工程项目的用户可以通过使用 NFS 文件系统（通常被称作 NFS 共享）中的一个挂载为 /myproject 的共享目录来存取该工程项目的文件。要存取共享的文件，用户进入各自机器上的 /myproject 目录。这种方法既不用输入口令又不用记忆特殊命令，就仿佛该目录位于用户的本地机器上一样。

3.8.2 挂载 NFS 文件系统

使用 mount 命令来挂载另一个机器上的 NFS 文件系统：

```
mount shadowman.example.com:/misc/export /misc/local
```

在这项命令中，shadowman.example.com 是 NFS 文件服务器的主机名；

/misc/export 是 shadowman 要导出的文件系统；/misc/local 是该文件系统在本地机器上的挂载位置。mount 命令运行之后（而且如果客户具有来自 shadowman.example.com NFS 服务器的正确权限的话），客户用户就可以执行 ls /misc/local 命令来显示 shadowman.example.com 上的 /misc/export 目录中的文件列表。

3.8.2.1 使用/etc/fstab 来挂载 NFS 文件系统

要挂载其它机器上的 NFS 共享的另一种方法是在 /etc/fstab 文件中添加一行。这一行中必须声明 NFS 服务器的主机名，要导出的目录，以及要挂载 NFS 共享的本地机器目录。你必须是根用户才能修改 /etc/fstab 文件。

/etc/fstab 中每行的一般语法如下所示：

```
server:/usr/local/pub    /pub    nfs    rsize=8192,wsize=8192,\

timeo=14,intr
```

挂载点 /pub 在客户机器上必须存在。在客户系统的 /etc/fstab 文件中把这一行添加完毕后，在 shell 提示下键入命令 mount /pub，以及将会从服务器中挂载的挂载点 /pub。

3.8.2.2 用 autofs 来挂载 NFS 文件系统

挂载 NFS 共享的第三种方法是使用 autofs。autofs 使用 automount 守护进程来管理你的挂载点，它只在文件系统被访问时才动态地挂载它们。

autofs 咨询主映射配置文件 /etc/auto.master 来决定要定义哪些挂载点。然后，它使用适用于各个挂载点的参数来启动 automount 进程。主映射配置中的每一行都定义一个挂载点，一个分开的映射文件定义在该挂载点下要挂载的文件系统。譬如，/etc/auto.misc 文件可能会定义 /misc 目录中的挂载点；这种关系在 /etc/auto.master 文件中会被定义。

auto.master 文件中的每个项目都有三个字段。第一个字段是挂载点。第二个字段是映射文件的位置，第三个字段可选。第三个字段可以包括超时数

值之类的信息。

譬如，要在你的机器上的 /misc/myproject 挂载点上挂载远程机器 penguin.example.net 上的 /project52 目录，在 auto.master 文件中添加以下行：

```
/misc   /etc/auto.misc --timeout 60
```

在 /etc/auto.misc 文件中添加以下行：

```
myproject -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.\
net:/proj52
```

/etc/auto.misc 中的第一个字段是 /misc 子目录的名称。该目录被 automount 动态地创建。它不应该在客户机器上实际存在。第二个字段包括挂载选项，如：rw 代表读写访问权。第三个字段是要导出的 NFS 的位置，包括主机名和目录。

autofs 是一种服务。要启动这项服务，在 shell 提示下，键入以下命令：

```
/sbin/service autofs restart
```

要查看活跃的挂载点，在 shell 提示下键入以下命令：

```
/sbin/service autofs status
```

如果你在 autofs 运行时修改了 /etc/auto.master 配置文件，你必须在 shell 提示下键入以下命令来通知 automount 守护进程重新载入配置文件：

```
/sbin/service autofs reload
```

3.8.2.3 使用 TCP

NFS 的默认传输协议是 UDP；然而，GTES10 内核提供了对通过 TCP 的 NFS 的支持。要通过 TCP 来使用 NFS，在客户系统上挂载 NFS 导出的文件系统时，包括一个 -o tcp 选项。例如：

```
mount -o tcp shadowman.example.com:/misc/export /misc/local
```

如果 NFS 挂载在 /etc/fstab 中被指定：

```
server:/usr/local/pub    /pub    nfs    rsize=8192,wsize=8192,\
timeo=14,intr,tcp
```

如果它在 autofs 配置文件中被指定：

```
myproject -rw,soft,intr,rsize=8192,wsize=8192,tcp penguin\
.example.net:/proj52
```

由于默认协议是 UDP，如果没有指定 -o tcp 选项，NFS 导出的文件系统就会通过 UDP 来进入。

使用 TCP 的优越性包括：

- 被提高了的连接持久性，因此获得的 NFS stale file handles 消息就会较少。
- 载量较大的网络的性能会有所提高。因为 TCP 确认每个分组，不像 UDP 只在完成时才确认。
- TCP 的拥塞控制技术比 UDP 要好（UDP 根本没有）。在一个拥塞情况严重的网络上，UDP 分组是被首先撤消的类型。这意味着，如果 NFS 正在写入数据（单元为 8K 的块），所有这 8K 数据都需要被重新传输。由于 TCP 的可靠性，8K 中只有一部分需要重新传输。
- 错误检测。当 tcp 连接中断（由于服务器停运），客户就会停止发送数据而开始进行重新连接。UDP 是无连接的，使用它的客户就会继续给网络发生数据直到服务器重新上线为止。

主要的不利因素是，由于 TCP 协议的费用，在性能方面的提高并不显著。

3.8.2.4 保留 ACL

Turbolinx DataServer 内核为 ext3 文件系统和使用 NFS 或 Samba 协议挂载的 ext3 文件系统提供了 ACL 支持。这样，如果某个 ext3 文件系统启用了 ACL，而且被 NFS 导出了，如果 NFS 客户能够读取 ACL，它们就能够被 NFS 客户使用。

3.8.3 导出 NFS 文件系统

从 NFS 服务器中共享文件又称导出目录。NFS 服务器配置工具可以用来把系统配置成 NFS 服务器。

要使用 NFS 服务器配置工具，你必须运行 X 窗口系统，具备根特权，并且安装了 system-config-nfs RPM 软件包。要启动这个程序，点击面板上的“主菜单 —> 系统设置 —> 服务器设置 —> NFS”，或键入 system-config-nfs 命令。

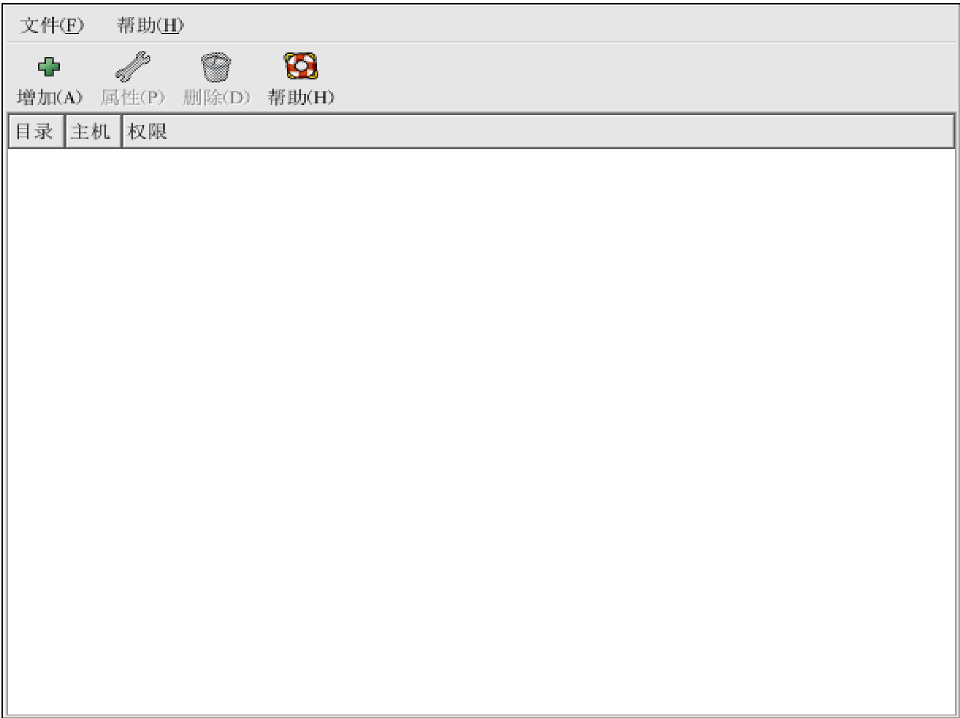


图 3-16 NFS 服务器配置工具

要添加 NFS 共享，点击“添加”按钮。如 图 3-17 所示的对话框会出现。

“基本”活页标签要求以下信息：

- 目录— 指定要共享的目录，如 /tmp。

- 主机 — 指定要共享目录的主机。
- 基本权限 — 指定目录应该有只读权限还是读写权限。



图 3-17 添加共享

“常规选项”活页标签允许你配置以下选项：

- 允许来自高于 1024 的端口的连接 — 在号码小于 1024 的端口上启动的服务必须以根用户身份启动。选择这个选项来允许根用户以外的用户来启动 NFS 服务。该选项和 insecure 相对应。
- 允许不安全的文件锁定 — 不需要锁定请求。该选项和 insecure_locks 相对应。
- 禁用子树检查 — 如果某文件系统的子目录被导出，但是整个文件系统没有被导出，服务器会检查所请求的文件是否在导出的子目录中。这种检查叫做子树检查（subtree checking）。选择这个选项来禁用子树检查。如果整个文件系统被导出，选择禁用子树检查可以提高传输率。该选项和 no_subtree_check 相对应。
- 按要求同步写操作 — 默认被启用，该选项不允许服务器在请求被写入磁盘前回复这些请求。该选项和 sync 相对应。如果它没有被选择，async 选项会被使用。
- 立即强制同步写操作 — 不推迟写入磁盘的操作。该选项和

no_wdelay 相对应。

“用户访问”活页标签允许你配置以下选项：

- 把远程根用户当作本地根用户 — 按照默认设置，根用户的用户 ID 和组群 ID 都是 0。根权限压缩（Root squashing）把用户 ID 0 和组群 ID 0 映射为匿名的用户和组群 ID，因此客户上的根用户就不会在 NFS 服务器上具备根特权。如果这个选项被选，根用户就不会被映射为匿名用户，客户上的根用户就会对导出的目录拥有根特权。选择这个选项会大大降低系统的安全 性。除非绝对必要，请不要选择它。该选项和 no_root_squash 相对应。
- 把所有客户用户当作匿名用户 — 如果该选项被选，所有用户和组群 ID 都会被映射为匿名用户。该选项和 all_squash 相对应。
- 为匿名用户指定本地用户 ID — 如果“把所有客户用户当作匿名用户”被选，这个选项会让 你为匿名用户指定一个用户 ID。该选项和 corresponds to anonuid 相对应。
- 为匿名用户指定本地组群 ID — 如果“把所有客户用户当作匿名用户”被选，这个选项会让 你为匿名用户指定一个组群 ID。该选项和 corresponds to anongid 相对应。

要编辑 NFS 共享，从列表中选择它，然后点击“属性”按钮。要删除某个现存 NFS 共享，从列表中选择它，然后点击“删除”按钮。

点击了“确定”来从列表中添加、编辑、或删除某个 NFS 共享后，改变就会立即生效 — 服务器守护进程被重新启动，原有的配置文件被保存为 /etc/exports.bak。新的配置文件被写入 /etc/exports。

NFS 服务器配置工具直接读写 /etc/exports 配置文件。因此，这个文件在使用该工具后可以被手工修改；手工修改了该文件后也可以使用这个工具（假定手工修改时使用了正确的语法）。

3.8.3.1 命令行配置

如果你更喜欢使用文本编辑器来编辑配置文件或者你没有安装 X 窗口系统，你可以直接修改配置文件。

/etc/exports 文件控制 NFS 服务器要导出哪些目录。它的格式如下：

```
directory hostname(options)
```

唯一需要指定的选项是 sync 和 async 之一（建议使用 sync is recommended）。如果指定了 sync，服务器在请求所做的改变被写入磁盘之前就不会回复这些请求。

例如：

```
/misc/export     speedy.example.com(sync)
```

会允许来自 speedy.example.com 的用户使用默认的只读权限来挂载 /misc/export，但是：

```
/misc/export     speedy.example.com(rw,sync)
```

将会允许来自 speedy.example.com 的用户使用读写权限来挂载 /misc/export。

在你每次改变 /etc/exports 的时候，你必须把改变通知给 NFS 守护进程，或使用以下命令来重新载入配置文件：

```
/sbin/service nfs reload
```

3.8.3.2 主机名格式

主机可以使用以下格式：

- 单个机器 — 一个全限定域名（能够被服务器解析的），主机名（能够被服务器解析的），或 IP 地址。

- 使用通配符来指定的机器系列 — 使用 * 或 ? 字符来指定一个字符串匹配。IP 地址中不使用通配符；不过如果反向 DNS 查询失败，它们可能会碰巧有用。在完整域名中指定通配符时，点（.）不包括在通配符中。例如：*.example.com 包括 one.example.com，但不包括 one.two.example.com.。

- IP 网络 — 使用 a.b.c.d/z，这里的 a.b.c.d 是网络，z 是子网掩码中的位数（如 192.168.0.0/24）。另一种可以接受的格式是 a.b.c.d/netmask，

这里的 a.b.c.d 是网络，netmask 是子网掩码（如 192.168.100.8/255.255.255.0）。

- Netgroups — 格式为 @group-name，这里的 group-name 是 NIS netgroup 的名称。

3.8.3.3 启动和停止服务器

在导出 NFS 文件系统的服务器上，nfs 服务必须在运行。

- 使用以下命令来查看 NFS 守护进程的状态：

```
/sbin/service nfs status
```

- 使用以下命令来启动 NFS 守护进程：

```
/sbin/service nfs start
```

- 使用以下命令来停止 NFS 守护进程：

```
/sbin/service nfs stop
```

- 要在引导时启动 nfs 服务，使用以下命令：

```
/sbin/chkconfig --level 345 nfs on
```

你还可以使用 chkconfig、ntsysv 或服务配置工具来配置要在引导时启动哪些服务。

3.9 Samba

Samba 使用 SMB 协议来通过网络连接共享文件和打印机。支持该协议的操作系统包括 Microsoft Windows、OS/2、和 Linux。

GTES10 内核包含对 ext3 文件系统的存取控制列表（Access Control List，ACL）支持。如果 Samba 服务器共享一个启用了 ACL 的 ext3 文件系统，而且客户系统的内核包含对从 ext3 文件系统读取 ACL 的支持，该客户就会自动识别和使用 ACL。

3.9.1 为什么使用 Samba

如果你的网络中既有 Windows 机器又有 Linux 机器，Samba 就会发挥作用。Samba 会允许文件和打印机被网络中的所有系统共享

3.9.2 配置 Samba 服务器

默认的配置文件（/etc/samba/smb.conf）允许用户把他们的主目录作为 Samba 共享来查看。它还把为系统配置的打印机作为 Samba 共享打印机来共享。换一句话说，你可以在你的系统上连接打印机，然后从网络上的 Windows 机器来打印。

3.9.2.1 图形化配置

要使用图形化界面来配置 Samba，使用 Samba 服务器配置工具。

Samba 服务器配置工具是用来管理 Samba 共享、用户、以及基本服务器设置的图形化界面。它修改 /etc/samba/ 目录中的配置文件。没有使用该程序进行的改变都会被保留。

要使用该程序，你必须在运行 X 窗口系统，具备根特权，并且安装了 system-config-samba RPM 软件包。要从桌面启动 Samba 服务器配置工具，点击面板上的“主菜单 —> 系统设置 —> 服务器设置 —> Samba”，或在 shell 提示（如 XTerm 或 GNOME 终端）下键入 system-config-samba 命令。



图 3-18 Samba 服务器配置工具

3.9.2.1.1 配置服务器设置

配置 Samba 服务器的第一步是配置服务器的基本设置和几个安全选项。启动了应用程序后，选择“首选项 —> 服务器设置”。“基本”活页标签如图 3-19 所示。



图 3-19 配置基本服务器设置

在“基本”标签上，指定计算机应在的工作组以及对计算机的简短描述。它们与 smb.conf 中的 workgroup 和 server string 选项相对应。

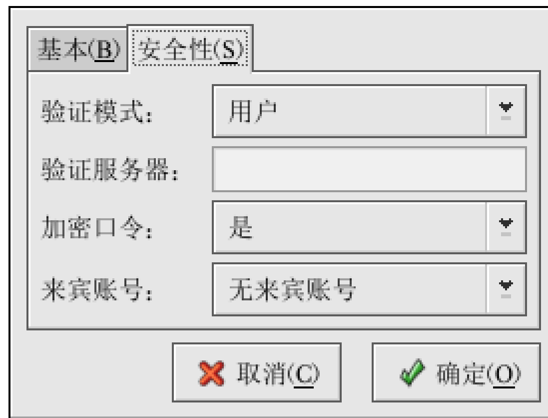


图 3-20 配置安全服务器设置

“安全性”标签包含以下选项：

- 验证模式 — 它和 security 选项相对应。选择以下验证模式中的一种。

- ADS — Samba 服务器充当活跃目录域（ADS）领域中的一个成员，Kerberos 在服务器上必须被安装和配置，并且 Samba 必须使用 net 工具成为 ADS 领域的一员。net 是 samba-client 软件包的一部分。该选项不会把 Samba 配置成一个 ADS 控制器。

- 域 — Samba 服务器依赖于 Windows NT 主要或备份域控制器来校验用户。服务器把用户名和口令传递给控制器，然后等待它们被返回。在“验证服务器”字段中指定主要或备份域控制器的 NetBIOS 名称。

如果“加密口令”选项被选，它必须被设置为“是”。

- 服务器 — Samba 服务器试图通过把用户名和口令组合传递给另一个 Samba 服务器来校验它们。如果它无法校验，服务器会试图使用用户验证模式来校验它们。在“验证服务器”字段中指定另一个 Samba 服务器的 NetBIOS 名称。

- 共享 — Samba 用户不必为每个 Samba 服务器都输入用户名和口令组合。它们在试图连接 Samba 服务器上的指定共享时才会被提示输入用户名和口令。

- 用户 — （默认）Samba 用户必须为每个 Samba 服务器提供一个有

效的用户名和口令。如果你想让“Windows 用户名”选项生效，选择这个选项。

- 加密口令 — 如果用户从 Windows 98、带有服务包 3 的 Windows NT 4.0、或其它最近版本的 Microsoft Windows 中连接，该选项必须被启用。口令在服务器和客户间使用加密格式而非可被截取的纯文本格式传输。它和 encrypted passwords 选项相对应。

- 来宾账号 — 当用户或来宾用户要登录入 Samba 服务器时，他们必须被映射到服务器上的有效用户。选择系统上的现存用户名之一作为来宾 Samba 账号。当用户使用来宾账号登录入 Samba 服务器，他们拥有和这个用户相同的特权。该选项和 guest account 选项相对应。

点击了“确定”后，所做改变会被写入配置文件，守护进程会被重新启动；因此改变会立即生效。

3.9.2.1.2 管理 Samba 用户

Samba 服务器配置工具要求在添加 Samba 用户之前，在充当 Samba 服务器的系统上必须存在一个活跃的用户账号。Samba 用户和这个现存的用户账号相关联。



图 3-21 管理 Samba 用户

要添加 Samba 用户，选择“首选项 —> Samba 用户”，然后点击“添加用户”按钮。在“创建新 Samba 用户”窗口中的本地系统上的现存用户列表中选择“Unix 用户名”。

如果用户在 Windows 机器上有一个不同的用户名，并将从 Windows 机器上登录入 Samba 服务器，请在“Windows 用户名”字段中指定 Windows 用户名。“服务器设置”首选项的“安全”活页上的“验证模式” 必须被设置为“用户”才能是这个选项生效。

你还需要为 Samba 用户配置一个“Samba 口令”，并再键入一次来确认这个口令。即便你选择了为 Samba 使用加密口令，仍建议你为所有用户设置一个不同于他们的系统口令的 Samba 口令。

要编辑某个现存用户，从列表中选择它，然后点击“编辑用户”。要删除某个现存的 Samba 用户，选择这个用户，然后点击“删除用户”按钮。删除 Samba 用户不会删除相关的用户账号。

点击了“确定”按钮后，用户就会被立即修改。

3.9.2.1.3 添加共享



图 3-22 添加共享

要添加共享，点击“添加”按钮。“基本”活页标签配置以下选项：

- 目录 — 通过 Samba 共享的目录。这个目录必须存在。
- 描述 — 对共享的简短描述。
- 基本权限 — 用户应该只能够读取共享目录中的文件还是应该能够读写共享目录中的文件。

在“访问”活页标签上，选择是否要只允许指定的用户来访问共享还是允许所有 Samba 用户来访问共享。如果你选择了要允许指定用户访问，从可用的 Samba 用户列表中选择这些用户。

点击了“确定”按钮后，共享就会立即被添加。

3.9.2.2 命令行配置

Samba 使用 /etc/samba/smb.conf 作为它的配置文件。如果你改变了这个配置文件，这个改变直到你使用 service smb restart 命令重启 Samba 守护进程后才会生效。

要指定 Windows 工作组和对它的简短描述，编辑 smb.conf 文件中的以下几行：

```
workgroup = WORKGROUPNAME

server string = BRIEF COMMENT ABOUT SERVER
```

把 WORKGROUPNAME 换成你的机器所属的 Windows 工作组名。BRIEF COMMENT ABOUT SERVER 是可选的，它被用作 Samba 系统的 Windows 注释。

要在你的 Linux 系统上创建 Samba 共享目录，在 smb.conf 文件中添加以下几行（根据你和你的系统需要修改了该文件之后）：

```
[sharename]

comment = Insert a comment here

path = /home/share/

valid users = tfox carole
```

```
public = no

writable = yes

printable = no

create mask = 0765
```

上面的例子允许用户 tfox 和 carole 从 Samba 客户中读写 Samba 服务器上的目录 /home/share。

3.9.2.3 加密口令

加密口令被默认启用，因为它更安全。如果加密口令没有被使用，纯文本口令就会被使用，它能够被别人使用网络分组嗅探器来截取。建议你使用加密口令。

Microsoft SMB 协议最初使用纯文本口令。然而，带有服务包 3 或更高的 Windows NT 4.0、Windows 98、Windows 2000、Windows ME、以及 Windows XP 要求加密的 Samba 口令。要在 Linux 系统和运行以上 Windows 操作系统的系统间使用 Samba，你可以编辑 Windows 注册器来使用纯文本口令或配置你的 Linux 系统的 Samba 来使用加密口令。如果你要修改注册器，你必须为所有 Windows 机器这么做 — 这很冒险，有可能导致进一步的冲突。为了更高的安全性，推荐你使用加密口令。

要配置 Samba 使用加密口令，遵循以下步骤：

- 为 Samba 创建一个单独的口令文件。要根据你的现存 /etc/passwd 文件来创建，在 shell 提示下键入以下命令：

```
cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
```

如果系统使用 NIS，键入以下命令：

```
ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
```

mksmbpasswd.sh 脚本和 samba 软件包一起被安装在你的 /usr/bin 目录上。

- 改变 Samba 口令文件的权限许可，因此只有根用户才有读写权限：

```
chmod 600 /etc/samba/smbpasswd
```

- 这个脚本不会把用户口令复制到新文件，Samba 用户账号在没有设置口令之前不会被激活。为了更高的安全性，建议你把用户的 Samba 口令设置为不同于用户的口令的口令。要设置每个 Samba 用户的口令，使用以下命令（把 username 替换为每个用户的用户名）：

```
smbpasswd username
```

- 加密口令必须被启用。由于它们被默认启用，它们不必在配置文件中被特别启用。不过，它们也不能在配置文件中被禁用。在 smb.conf 文件中，请确定以下行不存在：

```
encrypt passwords = no
```

如果它确实存在，请在行首加一个分号（;）来把它变成注释，这样该行就会被忽略，加密口令就会被启用。如果该行存在但没有被注释掉，请删除它或把它变成注释。

要在配置文件中特别启用加密口令，给 /etc/samba/smb.conf 文件添加以下几行：

```
encrypt passwords = yes

smb passwd file = /etc/samba/smbpasswd
```

- 在 shell 提示下键入 service smb restart 来确定 smb 服务被启动。
- 如果你想让 smb 服务被自动启动，使用 ntsysv、chkconfig、或服务配置工具来在运行时间启用它。

当使用了 passwd 命令后，pam_smbpass PAM 模块能够被用来同步用户的 Samba 口令和他们的系统口令。如果用户引发了 passwd 命令，他用来登录到 GTES10 系统的口令以及他要连接 Samba 共享所必须提供的口令就会被改变。

要启用这个功能，把以下行添加到 /etc/pam.d/system-auth 的 pam_cracklib.so 之下：

```
password required /lib/security/pam_smbpass.so nullok use_authtok
try_first_pass
```

3.9.2.4 启动和停止服务器

在通过 Samba 共享目录的服务器上必须运行 smb 服务。

- 使用以下命令来查看 Samba 守护进程的状态：

```
/sbin/service smb status
```

- 使用以下命令来启动守护进程：

```
/sbin/service smb start
```

- 使用以下命令来停止守护进程：

```
/sbin/service smb stop
```

- 要在引导时启动 smb 服务，使用以下命令：

```
/sbin/chkconfig --level 345 smb on
```

你还可以使用 chkconfig、ntsysv 或服务配置工具来配置要在引导时启动哪些服务。

3.9.3 连接 Samba 共享

你还可以使用 Nautilus 来查看你的网络上的可用 Samba 共享。选择面板上的“主菜单 —> 网络服务器”来查看你的网络上的 Samba 工作组的列表。你还可以在 Nautilus 的“位置：”栏里键入 smb: 来查看工作组。

如图 3-23 所示，在网络上每个可用 SMB 工作组旁边都会出现一个图标。

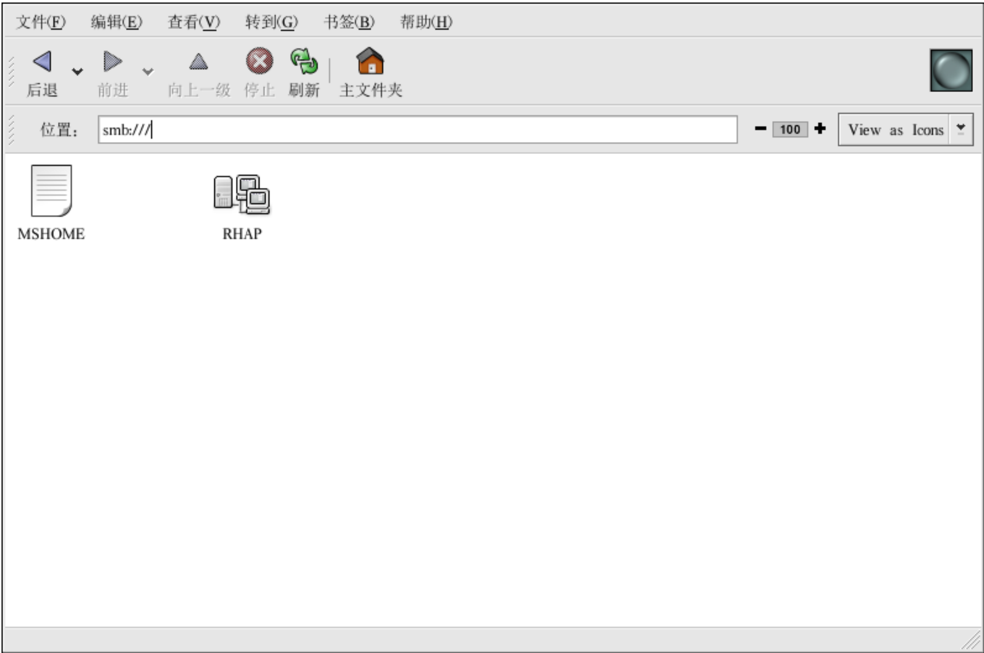


图 3-23 Nautilus 中的 SMB 工作组

双击工作组图标之一来查看那个工作组内的计算机的列表。

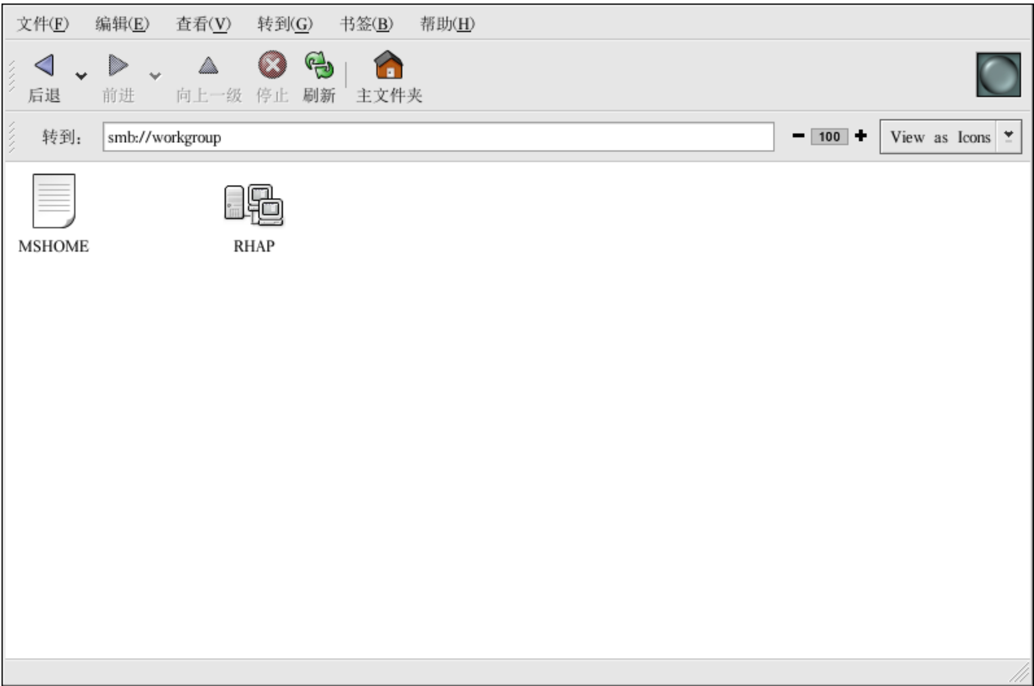


图 3-24 Nautilus 中的 SMB 机器

如你在图 3-24 中所见，工作组内每个机器都有一个图标。双击某个图标来查看该机器上的 Samba 共享。如果需要用户名和口令组合，你会被提示输入它们。

你也可以在 Nautilus 的“位置：”栏内使用以下语法（把 <servername> 和 <sharename>替换成相应值）来指定 Samba 服务器和共享名称：

```
smb://<servername>/<sharename>/
```

3.9.3.1 命令行

要查询网络上的 Samba 服务器，使用 findsmb 命令。每个找到的服务器都会显示其 IP 地址、NetBIOS 名称、工作组名称、操作系统、以及 SMB 服务器版本。

要连接 Samba 共享，从 shell 提示下，键入以下命令：

```
smbclient //<hostname>/<sharename> -U <username>
```

把 <hostname> 替换为你想连接的 Samba 服务器的主机名或 IP 地址，把 <sharename> 替换为你想浏览的共享目录的名称，把 <username> 替换成系统的 Samba 用户名。输入正确的口令或按 [Enter] 键（若不要求该用户的口令）。

如果你看到了 smb:\> 提示，这说明你已成功登录。登录后，键入 help 来获得一个命令列表。如果你想浏览你的主目录的内容，把 sharename 替换成你的用户名。如果没有使用 -U 选项，当前用户的用户名就会被传递给 Samba。

要退出 smbclient，在 smb:\> 提示下键入 exit。

3.9.3.2 挂载共享

有时，你可能想把 Samba 共享挂载到目录上，这样该目录内的文件就如同是本地文件系统的一部分。

要把 Samba 共享挂载到某目录中，若该目录不存在则创建它，然后以根用户身份执行以下命令：

```
mount -t  smbfs -o username=<username> //<servername>/<sharename>
/mnt/point/
```

该命令会把 <servername> 中的 <sharename> 挂载在本地的 /mnt/point/ 目录中。

3.10 动态主机配置协议（DHCP）

动态主机配置协议（DHCP）是用来自动给客户机器分配 TCP/IP 信息的网络协议。每个 DHCP 客户都连接到位于中心的 DHCP 服务器，该服务器会返回包括 IP 地址、网关和 DNS 服务器信息的客户网络配置。

3.10.1 为什么使用 DHCP

DHCP 在快速发送客户网络配置方面很有用场。当配置客户系统时，若管理员选择了 DHCP，他就不必输入 IP 地址、子网掩码、网关、或 DNS 服务器。客户从 DHCP 服务器中检索这些信息。DHCP 在管理员想改变大量系统的 IP 地址时也大有用途。与其重新配置所有系统，管理员只需编辑服务器上的一个用于新 IP 地址集合的 DHCP 配置文件即可。如果某机构的 DNS 服务器改变了，这种改变只需在 DHCP 服务器上而不必在 DHCP 客户上进行。一旦客户的网络被重新启动（或客户重新引导系统），改变就会生效。

除此之外，如果便携电脑或任何类型的可移计算机被配置使用 DHCP，只要每个办公室都有一个允许它联网的 DHCP 服务器，它就可以不必重新配置而在办公室间自由移动。

3.10.2 配置 DHCP 服务器

要配置 DHCP 服务器，请修改配置文件 /etc/dhcpd.conf。

DHCP 还使用 /var/lib/dhcp/dhcpd.leases 文件来贮存客户租期数据库。

3.10.2.1 配置文件

配置 DHCP 服务器的第一步是创建贮存客户网络信息的配置文件。全局选项可以为所有客户声明，可选选项可以为每个客户系统声明。

该配置文件可以使用任何附加的制表符或空行来进行简单格式化。关键字是区分大小写的，起首为井号（#）的行是注释。

目前实现了两种 DNS 更新方案 — 特殊 DNS 更新模式和过渡性 DHCP-DNS 互动草图更新模式。如果这两种模式被接受为 IETF 标准进程的一部分，就会出现第三个模式 — 标准 DNS 更新方法。DHCP 服务器必须配置使用这两种当前方案中的一种。版本 3.0b2pl11 以及更早的版本使用特殊模式；不过，这种模式已经过时。如果你想保留相同的行为方式，在配置文件的开头添加以下一行：

```
ddns-update-style ad-hoc;
```

要使用推荐的模式，在配置文件的开头添加以下一行：

```
ddns-update-style interim;
```

配置文件中有两类陈述：

- 参数 — 表明如何执行任务，是否要执行任务，或将哪些网络配置选项发送给客户。
- 声明 — 描述网络的布局；描述客户；提供客户的地址；或把一组参数应用到一组声明中。

某些参数必须以 option 关键字开头，它们也被称为选项。选项配置 DHCP 的可选选项；而参数配置的是必选的或控制 DHCP 服务器行为的值。

在使用大括号（{ }）的部分之前声明的参数（包括选项）通常被当做全局参数。全局参数应用位于其下的所有部分。

在下例中，routers、subnet-mask、 domain-name、domain-name-servers 和 time-offset选项被用于所有在它们下面声明的 host 声明中。

如下例所示，你可以声明 subnet。你必须为你的网络中的每一个子网包括一个 subnet 声明，否则，DHCP 服务器可能无法启动。

在这个例子中，子网中的每个 DHCP 客户都带有全局选项，并且声明了 range。客户被分配给 range 之内的 IP 地址。

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.254;
        option subnet-mask              255.255.255.0;
        option domain-name              "example.com";
        option domain-name-servers       192.168.1.1;
        option time-offset       -18000;  # Eastern Standard Time
        range 192.168.1.10 192.168.1.100;
}
```

所有共享同一物理网络的子网应该在 shared-network 声明之内声明，如下例所示。在 shared-network 之内，但在被包围起来的 subnet 声明之外的参数被当做全局参数。shared-network 的名称应该是对网络有描述性的标题，例如，使用 test-lab 来描述所有处于实验室（test lab）环境中的子网。

```
shared-network name {
    option domain-name            "test.turbolinux.com.cn";
    option domain-name-servers  ns1.turbolinux.com.cn, \
ns2.turbolinux.com.cn;
    option routers               192.168.1.254;
    more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.1 192.168.1.31;
    }
    subnet 192.168.1.32 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.33 192.168.1.63;
    }
}
```

如下 例中所演示，group 声明可以用来把全局参数应用到一组声明中。例如，你可以组合共享的网络、子网、主机或其它组群。

```
group {
   option routers               192.168.1.254;
   option subnet-mask           255.255.255.0;
   option domain-name           "example.com";
   option domain-name-servers    192.168.1.1;
```

```
   option time-offset       -18000;     # Eastern Standard Time
   host apex {
      option host-name "apex.example.com";
      hardware ethernet 00:A0:78:8E:9E:AA;
      fixed-address 192.168.1.4;
   }
}
```

要配置将动态 IP 地址租给子网内系统的 DHCP 服务器,用你的数值来修改下 例。它为客户声明一个默认租期、最长租期、以及网络配置值。范例中把 range 192.168.1.10 和 192.168.1.100 之间的 IP 地址分配给客户。

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";
subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.10 192.168.1.100;
}
```

要根据网卡的 MAC 地址给客户分配 IP 地址，使用 host 声明内的 hardware ethernet 参数。 如下 例中所演示，host apex 声明表明：网卡的 MAC 地址为 00:A0:78:8E:9E:AA 的系统所分配的 IP 地址将一直是 192.168.1.4。

注意，你还可以使用可选的参数 host-name 来为客户分配主机名。

```
host apex {
```

```
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    fixed-address 192.168.1.4;
}
```

3.10.2.2 租期数据库

在 DHCP 服务器上，/var/lib/dhcp/dhcpd.leases 文件中存放着 DHCP 的客户租期数据库。该文件不应该被手工修改。每个新近分配的 IP 地址的 DHCP 租期信息都会自动储存在租期数据库中。该信息 包括租期的长度；IP 地址被分配的对象；租期的开始和终止日期； 以及用来检索租期的网卡的 MAC 地址。

租期数据库中所用的时间是格林威治标准时间（GMT），不是本地时间。

租期数据库不时被重建，因此它不算太大。首先，所有已知的租期会被储存到一个临时的租期数据库中， dhcpd.leases 文件被重命名为 dhcpd.leases~，然后，临时租期数据库被写入 dhcpd.leases 文件。

在租期数据库被重命名为备份文件，新文件被写入之前，DHCP 守护进程有可能被杀死，系统也有可能会崩溃。如果发生了这种情况，dhcpd.leases 文件不存在，但它却是启动服务所必需的。这时，请不要创建新租期文件。因为这样做会丢失所有原有的旧租期文件，从而导致更多问题。正确的办法是把 dhcpd.leases~ 备份文件重命名为 dhcpd.leases，然后再启动守护进程。

3.10.2.3 启动和停止服务器

要启动 DHCP 服务，使用 /sbin/service dhcpd start 命令。要停止 DHCP 服务，使用 /sbin/service dhcpd stop 命令。

如果你的系统连接了不止一个网络接口，但是你只想让 DHCP 服务器启动其中之一，你可以配置 DHCP 服务器只在那个设备上启动。在 /etc/sysconfig/dhcpd 中，把接口的名称添加到 DHCPDARGS 的列表中：

```
# Command line options here
DHCPDARGS=eth0
```

如果你有一个带有两个网卡的防火墙机器，这种方法就会大派用场。一个网卡可以被配置成 DHCP 客户来从互联网上检索 IP 地址;另一个网卡可以被用作防火墙之后的内部网络的 DHCP 服务器。仅指定连接到内部网络的网卡使系统更加安全，因为用户无法通过互联网来连接它的守护进程。

其它可在 /etc/sysconfig/dhcpd 中指定的命令行选项包括：

-p <portnum> — 指定 dhcpd 应该监听的 udp 端口号码。默认值为 67。DHCP 服务器在比指定的 udp 端口大一位的端口号码上把回应传输给 DHCP 客户。譬如，如果你使用了默认的端口 67，服务器就会在端口 67 上监听请求，然后在端口 68 上回应客户。如果你在此处指定了一个端口号码，并且使用了 DHCP 转发代理，你所指定的 DHCP 转发代理所监听的端口就必须是同一端口。

- -f — 把守护进程作为前台进程运行。这在调试时最常用。
- -d — 把 DCHP 服务器守护进程记录到标准错误描述器中。这在调试时最常用。如果它没有指定，日志将被写入 /var/log/messages。
- -cf <filename> — 指定配置文件的位置。默认位置是 /etc/dhcpd.conf。
- -lf <filename> — 指定租期数据库文件的位置。如果租期数据库文件已存在，在 DHCP 服务器每次启动时使用同一个文件至关重要。强烈建议你只在无关紧要的机器上为调试目的才使用该选项。默认的位置是 /var/lib/dhcp/dhcpd.leases。
- -q — 在启动该守护进程时，不要显示整篇版权信息。

3.10.2.4 DHCP 转发代理

DHCP 的转发代理（dhcrelay）允许你把无 DHCP 服务器的子网内的 DHCP 和 BOOTP 请求转发给其它子网内的一个或多个 DHCP 服务器。

当某个 DHCP 客户请求信息时，DHCP 转发代理把该请求转发给 DHCP

转发代理启动时所指定的一列 DHCP 服务器。当某个 DHCP 服务器返回一个回应 时，该回应被广播或单播给发送最初请求的网络。

除非使用 INTERFACES 指令在 /etc/sysconfig/dhcrelay 文件中指定了接口，DHCP 转发代理监听所有接口上的 DHCP 请求。

要启动 DHCP 转发代理，使用 service dhcrelay start 命令。

3.10.3 配置 DHCP 客户

配置 DHCP 客户的第一步是确定内核能够识别网卡。多数网卡会在安装过程中被识别，系统会为该卡配置使用恰当的内核模块。如果你在安装后添加了一张网卡，Kudzu[1] 应该会识别它，并提示你为它配置相应的内核模块。

要手工配置 DHCP 客户，你需要修改 /etc/sysconfig/network 文件来启用联网；并修改 /etc/sysconfig/network-scripts 目录中每个网络设备的配置文件。在该目录中，每个设备都应该有一个叫做 ifcfg-eth0 的配置文件，这里的 eth0 是网络设备的名称。

/etc/sysconfig/network 文件应该包含以下行：

```
NETWORKING=yes
```

如果你想在引导时启动联网，NETWORKING 变量必须被设为 yes。

/etc/sysconfig/network-scripts/ifcfg-eth0 文件应该包含以下几行：

```
DEVICE=eth0

BOOTPROTO=dhcp

ONBOOT=yes
```

每个你想配置使用 DHCP 的设备都需要一个配置文件。

其它网络脚本的选项包括：

• DHCP_HOSTNAME — 只有当 DHCP 服务器在接收 IP 地址前需要客户指定主机名的时候才使用该选项。（GTES10 中的 DHCP 服务器守护进程不支持该功能。）

- PEERDNS=<answer>，这里的<answer> 是以下之一：

yes — 使用来自服务器的信息来修改 /etc/resolv.conf。若使用 DHCP，那么 yes 是默认值。

no — 不要修改 /etc/resolv.conf。

- SRCADDR=<address>，这里的<address> 是用于输出包的指定源 IP 地址。

- USERCTL=<answer>，这里的<answer> 是以下之一：

yes — 允许非根用户控制该设备。

no — 不允许非根用户控制该设备。

3.11 Apache HTTP 服务器配置

GreatTurbo Enterprise Server 10 为用户提供功能强大的 Apache HTTP 服务器，新的 Apache 服务器基于最新的 2.0 版本，可以为用户提供稳定高效的 HTTP 服务，并最大程度的减轻了系统管理的压力。

如果需要 HTTP 服务以及配置工具，请确认系统内安装了 httpd 和 system-config-httpd 两个软件包。同时系统需要安装 X Window 系统，以便配置工具能够运行。

在图形环境下，请在主菜单中选择 System Settings，在子菜单中选择 Server Settings 中的 HTTP。如果处于控制台中，键入命令 system-config-httpd 也可以进入配置工具。

新版本的 Apache 服务器使用/etc/httpd/conf/httpd.conf 文件作为配置文件。

当配置工具界面启动以后，可以遵循以下 8 个步骤进行配置。

- 在 main 页面中进行基本设置。
- 在 virtual host 页面中进行默认的设置。
- 在 virtual host 页面中配置默认的虚拟主机。

- 如果需要配置多虚拟主机或者多 URL，可以按照需求进行增加。
- 在 Server 页面中进行服务器配置。
- 在 performance turing 页面中进行连接等设置。
- 将所有必要的文件复制到 DocumentRoot 和 cgi-bin 目录下。
- 保存工具信息，退出配置工具。

3.11.1 基本设置

配置工具中的 main 页面图 3-25 所示。



图 3-25 Apache 基本设置

请在服务器名文本框中输入服务器名称，这里的名称对应于配置文件中的 ServerName 项，该项设置了 web 服务器的主机名称。

在网主电子邮件地址文本框中输入服务器维护人的邮件地址。这里的内容对应于配置文件中的 ServerAdmin 项。可以配置错误页面，并将这个邮件地址放置到错误页面上，以便用户将错误报告给服务器管理员。

在 Available Addresses 区域可以定义服务器所监听的端口。这里的设置对应于配置文件中的 Listen 项。GreatTurbo Enterprise Server 10 设置的默认端口是 80。可以选择 Add 按钮增加新的监听端口，如果选择 Add 按钮，出现如图 3-26 中所示的配置界面。



图 3-26 添加新地址

如果选择监听所有地址选项，则服务器会在指定的端口上监听所有的 IP 地址。或者在地址中指定监听的 IP 地址。如果在地址中输入星号（＊），效果和选择监听所有地址选项相同。

如果选择 Edit 按钮，可以对选定的项进行重新编辑。选择 Delete 则会删除选定的项。

3.11.2 默认设置

选择虚拟主机页面，点击编辑默认设置按钮，出现如图 3-27 所示的配置窗口。在这个页面中，可以进行一些默认的配置。

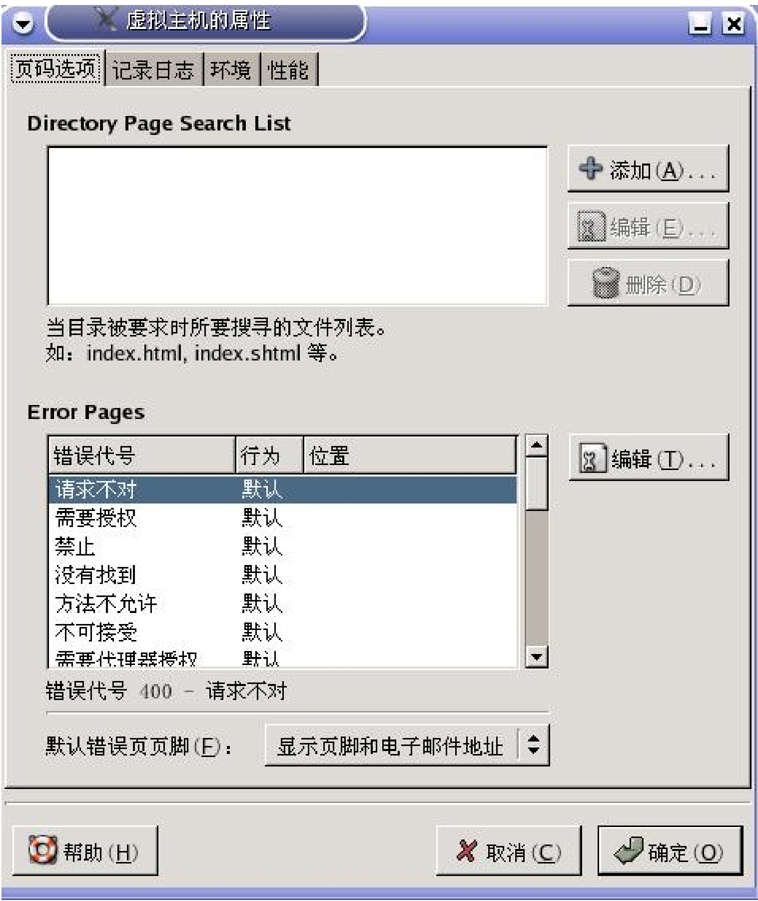


图 3-27 虚拟主机属性—页码选项

3.11.2.1 页码选项配置

Directory Page Search List 区域对应于配置文件中的 DirectoryIndex 项。在用户指定访问相应路径的时候，DirectoryIndex 中的内容将会被使用。

例如，如果用户访问了 http://www.test.com/dir/，则服务器会在 DirectoryIndex 中所列出的目录中选择一个文件返回给用户。通常会是 index.html 这样的文件。

在 Error Page 部分，可以配置出错页面，访问出错的时候，可以重定向到

指定的错误页面上去，这个选项对应于配置文件中的 ErrorDocument 项中。如果系统出错或者用户连接出现问题的时候，那么相应的出错信息就会显示给用户。这些出错信息都列在了错误代号这一栏。点击编辑按钮可以对这些信息进行重新编辑。编辑窗口中的行为中列出了三种方式。

- 默认方式：系统在出错的时候会显示系统默认的信息。
- URL 方式：系统出错时将用户重定向到指定的 URL，在 Location 编辑框中输入重定向的 URL 地址。
- 文件方式：系统出错时将用户重定向到指定的文件，在 Location 编辑框中输入重定向的文件。

例如，如果需要重新定向 404 Not Found 这个错误到一个文件 404.html，则首先将该文件复制到 DocumentRoot 目录下，该目录是用户定义的文档目录，稍后还会有介绍，默认的 DocumentRoot 是/var/www/html/。然后选择 404 Not Found 错误号进行编辑，在 Behavior 中选择 File，在 Location 框中输入 html/404.html。

在默认错误页页脚选项中，有三个选项。

- 显示页脚和邮件地址：在错误页的页脚显示网站维护者的邮件地址。也就是在 ServerAdmin 项中的信息，稍后会进行进一步的解释。
- 显示页脚：显示默认的页脚
- 无页脚：不显示页脚。

3.11.2.2 记录日志

记录日志页面配置传输日志和错误日志，默认情况下，服务器将传输日志写到 /var/log/httpd/access_log 日志文件中，将错误日志写到 /var/log/httpd/error_log 日志文件中。



图 3-28 虚拟主机属性－记录日志

Transfer Log 记录了所有的试图进行连接的信息。这些信息中包含尝试连接的用户的 IP 地址，尝试的时间以及尝试连接哪些文件等。可以在记录到文件选项中输入新的日志文件名称以替换默认的日志文件。这里的选项对应了配置文件中的 TransferLog 项。

也可以选择使用定制记录设施来自行定义日志字符串，这里的选项对应配置文件中的 Custom Log String 项。

错误日志记录了服务器所有的出错信息，同样也可以按照传输日志的步骤进行错误日志的配置。

日志级别选项定义了各种错误的级别，该选项对应配置文件中的 LogLevel 项，

逆向 DNS 查寻选项对应于配置文件中的 HostnameLookups，有以下三种选择：

- 逆向查寻：对于每一个用户的连接，服务器都将对用户的 IP 进行 DNS 搜索，以便得到用户的主机名称。
- 双重逆向查寻：对于每一个用户的连接，服务器不但要对用户的 IP 进行 DNS 搜索，得到用户的主机名称，还要对得到的主机名称进行反向搜索，用户的 IP 必须和反向搜索得到的 IP 列表中的一个相同。
- 无逆向查寻：不进行任何 DNS 搜索。

进行 DNS 搜索是消耗网络资源比较大的操作，默认选项推荐不使用 DNS 搜索。

3.11.2.3 环境设置

环境页面用来为 CGI 配置各种环境变量。有以下三种配置区域。在这些配置区域可以使用添加,编辑,删除按钮来增加，编辑和删除各种环境变量。



图 3-29 虚拟主机属性—环境

- 使用 Set for CGI Scripts 配置选项配置传递给 CGI 和 SSI 页面的变量，例如，如果需要将环境变量 MAXNUM 设置为 50，可以点击 Add 按钮，分别将 MAXNUM 和 50 填入相应的文本框，选择 OK 即可。该选项对应配置文件的 SetEnv 项。

- 当服务器第一次启动执行 CGI 的时候，会使用到 Pass to CGI Scripts 区域配置的环境变量的值，该选项对应配置文件中的 PassEnv。

- 如果需要删除某个环境变量，可以在 Unset for CGI Scripts 区域进行配置，该选项对应配置文件中的 UnsetEnv。

3.11.2.4 性能调整

性能页面用来配置各种目录的选项。在配置文件中对应于 Directory 项。

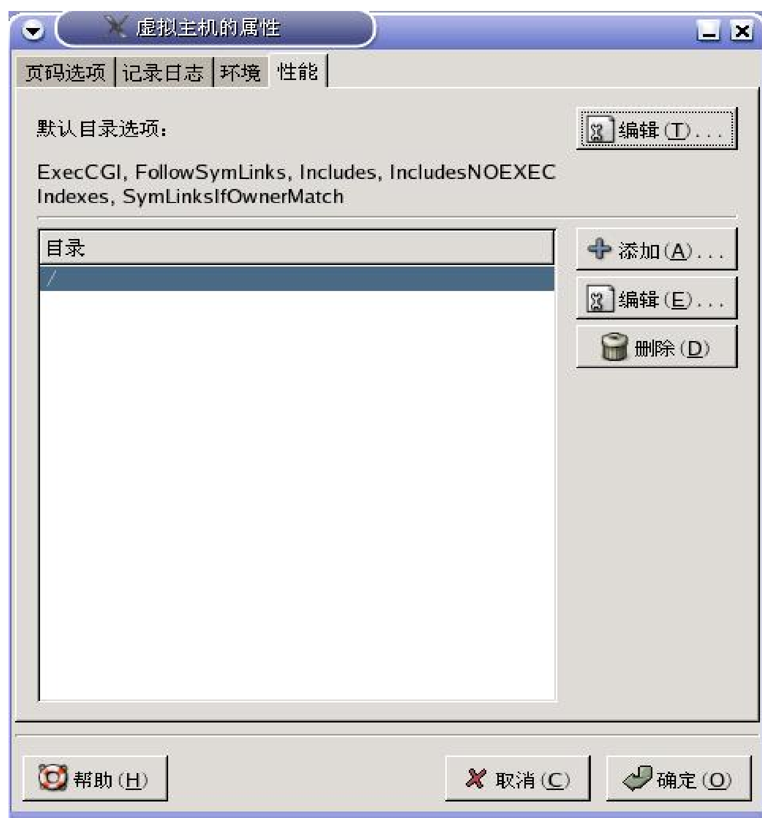


图 3-30 虚拟主机属性—性能

选择右上角的编辑按钮会配置默认目录选项，这些选项会对除了列在页面下方表中的目录之外的所有目录都起效。这些选项包含如下的内容：

- ExecCGI：如果不选择该项，则所有的 CGI 脚本都不会被执行。
- FollowSymLinks：是否允许对符号连接进行跟进操作。
- Includes：是否允许服务器端的包含。
- IncludesNOEXEC：允许服务器端的包含，但是在脚本中禁止#exec 和#include。

- Indexes：如果在某个目录中不包含 index.html 这样的指示页面，系统为用户提供一个默认的规整的页面显示。

- Multiview：提供多层显示。

- SymLinksIfOwnerMatch：如果一个符号连接的源和目标同属于一个拥有者，则允许跟进符号连接。

如果需要对某个特定的目录进行配置，点击添加按钮进入配置界面。在 Directory 文本编辑框中输入要配置的目录。如果选定了让 .htaccess 文件取代目录选项选项，在目录.htaccess 中的配置文件优先得到执行。在 Order, Deny List，Allow List 区域中分别可以进行用户访问权限顺序设置，拒绝访问列表地址设置和允许访问地址列表设置。

3.11.3 虚拟主机设置

虚拟主机功能可以允许用户对于不同的 IP 地址，不同的主机名，不同的端口运行不同的服务器，也可以使得不同的主机名称对应相同的服务器。例如，可以设置 http://www.example.com 和 http://www.anotherexample.com 运行于同一个 web 服务器上。如果没有指定虚拟主机的属性，那么就认为使用默认的配置属性。GreatTurbo Enterprise Server 10 提供了一个默认的虚拟主机，用户也可以自行增加虚拟主机并对其进行配置。

- 增加和编辑虚拟主机

如果想增加新的虚拟主机，点击添加按钮，如果想编辑现有的虚拟主机，选中想编辑的虚拟主机的名称并点击 Edit 按钮。

- 常规选项

通用配置页面设置虚拟主机的基本信息。虚拟主机名表明该虚拟主机的名称。文档根目录设置根文档的目录，通常这个目录里有一个 index.html 文件。该选项对应配置文件中的 DocumentRoot 项。默认的根文档目录是 /var/www/html。

在 Host Information 项，有以下三种选项。

- 默认虚拟主机：系统中只能配置一个默认虚拟主机，如果一个请求的

IP 不在其它任何的虚拟主机中，默认虚拟主机将会被使用。

- 基于 IP 的虚拟主机：如果想配置多余一个的 IP 地址，可以使用空格进行分隔。如果需要指定端口，请使用 IP：Port 格式。

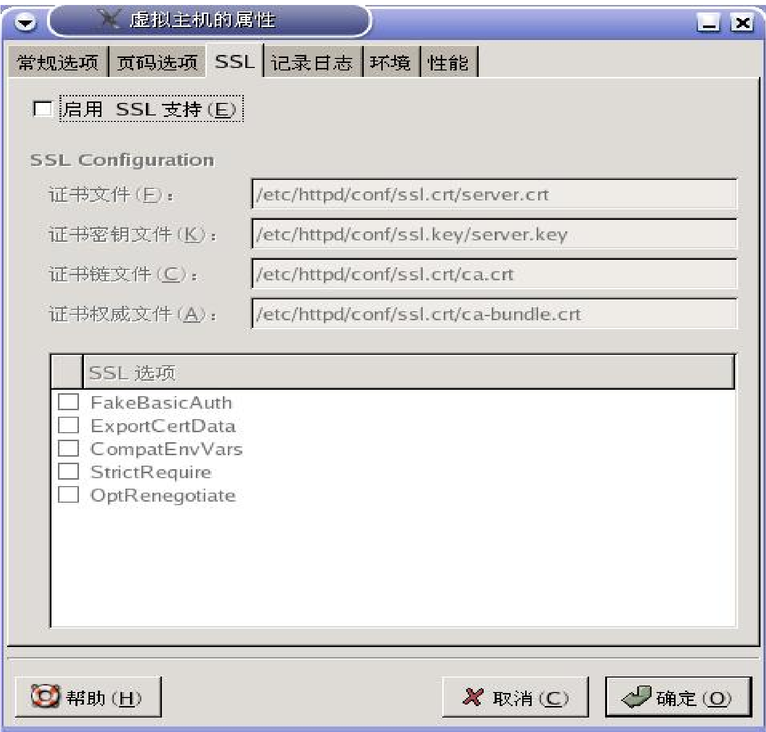
- 基于名称的虚拟主机：如果想配置多余一个的 IP 地址，可以使用空格进行分隔。如果需要指定端口，请使用 IP：Port 格式。在服务器主机名称文本框中输入虚拟主机的名称，如果想添加，编辑，删除主机的别名，可以分别点击别名框边的相应按钮。



图 3-31 虚拟主机属性－常规选项

3.11.3.1.1 SSL

请注意，当使用 SSL 的时候，不能使用基于名称的虚拟主机。这是因为 SSL 的握手协议先于 HTTP 请求，而主机名则是通过 HTTP 请求来得到的，因此，如果使用基于名称的虚拟主机类型的虚拟主机，则只能使用非 SSL



方式。

图 3-32 虚拟主机属性－SSL

如果服务器没有配置成为 SSL 类型的，则服务器与客户端之间的请求不进行加密。不同的用户需要不同的服务类型，例如对于分发升级软件包的站点，不需要 SSL 设置，但是对于商业站点，则 SSL 是必不可少的。

如果需要使用 SSL 功能，首先必须在主菜单页面中的 Basic Setup 上打开 443 端口。然后选中启用 SSL 支持。SSL Configuration 部分是一个预先配置好的模拟的数字证书系统，如果网站用作商业用途，请购买一个 CA 的数字证书。

3.11.3.1.2 其它选项

剩余的配置页面和点击编辑默认选项按钮所示的一样，配置方法也类似。

3.11.4 服务器设置

服务器页面可以对服务器进行一些基本的配置。

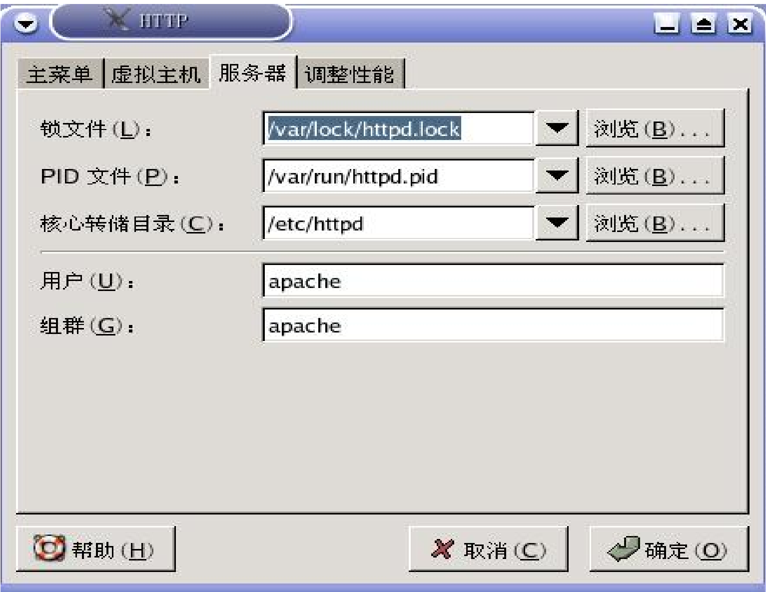


图 3-33 HTTP 设置 一服务器

- 锁文件对应配置文件中的 LockFile 项，这个文件必须存储在本地硬盘上，一般不要修改系统给定的默认值。如果需要改动，请确保给出的文件路径在本地硬盘上，并且该文件可以被 root 用户读取。

- PID 文件对应配置文件中的 PidFile 项，它包含了 Apache 服务器启动以后所对应的进程号，通常不要改动这里的默认设置。

- 核心转储目录对应配置文件中的 CoreDumpDirectory 项，当 Apache 系统发生了系统崩溃的时候，会使用到这个目录来保存崩溃信息，以便于找

到崩溃原因。请确认输入的目录对于服务器运行者是可写的。

- 用户选项对应配置文件中的 User 项，Apache 系统会使用该项所指定的用户 ID 来确定用户的读写权限，这里的设定决定了服务器对于文件系统的访问权限，这个权限对于访问 Apache 服务器的用户也是一样的。默认的用户是 apache。

- 组选项对应于配置文件中的 Group 项，该配置类似与 User 项，它表明了服务器是在那个用户组的权限下应答用户的请求。默认的 Group 也是 apache。

3.11.5 性能调整

调整性能页面为用户提供了性能调整的手段，可以设定最大服务器子进程数量，最大用户连接数等参数。



图 3-34 HTTP 设置—调整性能

- 最多连接数选项对应配置文件中的 MaxClients 项，对于每一个用户连接，Apache 服务器都启动一个子程序相对应，用户可以指定最大容许的数量，当超出这个数值的时候，服务器会拒绝后到的连接请求。
- 连接超时选项对应配置文件中的 TimeOut 项，它定义了数据传输过程中服务器最大的等待时间，当超过这个时限的时候，系统会认为传输失败。
- “每次连接最多请求数量”选项对应配置文件中的 MaxRequestsPerChild 项，它表明了每一个子服务器最大能够相应的请求数量。如果选取“允许每次连接可有无限此要求”，则连接的请求数量没有限制。
- “允许持久性的连接”选项对应于配置文件中的 KeepAlive 项，“下次连接的超时时间”选项对应配置文件中的 KeepAliveTimeout 项。

3.11.6 保存设定

如果不想保存设定，点击窗口下方的取消按钮，如果保存请点击确定按钮。在弹出的对话框中会再次询问以便确认是否真的要执行取消或者保存操作。

请注意，在保存了新的设置以后，需要执行 serive httpd restart 命令以便重新激活 Apache 服务器。

3.12 Apache HTTP 安全服务器配置

3.12.1 简介

Apache 服务器可以通过 mod_ssl 模块来使用 OpenSSH 库以及工具包，从而构建一个安全的网络服务环境。

mod_ssl 是 Aapche 提供的一个很重要的模块，它可以利用 OpenSSH 等工具包为网络连接提供一个加密的环境，防止信息内容在网络上的泄露。

mod_ssl 缺省的配置文件在/etc/httpd/conf.d/ssl.conf 中，为了能够是 Apache

能够使用 mod_ssl 模块，必须在 Aapche 的配置文件/etc/httpd/conf/httpd.conf 中加入 Include conf.d/*.conf 这样的语句，将 mod_ssl 的配置文件包含进 Apache 的配置文件。

3.12.2 与安全相关包的简介

为了建立安全服务器，至少需要以下的软件包

- httpd：包中包含了服务器的运行程序，帮助文件等。
- mod_ssl：它通过 SSL 和 TLS 来为上层软件提供加密算法。
- openssl：它实现了 SSL 和 TLS 协议，作为安全系统的底层库来使用。
- httpd-devel：提供了 httpd 的开发库和头文件。
- httpd-manual：提供了 html 格式的 Apache 的文档。
- OpenSSH 程序组：这个程序组包含了若干个包，它们共同提供了一套安全网络连接方式。其中 openssh 提供了 ssh 这样的远程登录程序。
- openssl-devel：提供 openssl 的开发库以及头文件等。
- stunnel：提供了基于 SSL 协议的 socket 接口服务。为上层软件利用 SSL 进行网络编程提供了方便。

3.12.3 安全与认证简介

安全服务器使用安全套接字层（SSL）和（多数情况下）来自证书权威（CA）的数字证书的组合来提供安全性。SSL 处理浏览器和安全服务器间的加密通讯和互相验证。CA 认可的数字证书为安全服务器提供验证。

加密依赖于钥匙的使用（你可以把它们当做数据格式的秘密编码和解码钥匙）。传统的或对称的加密术中，事务的两端都使用同一把钥匙，它们可以用这把钥匙来破译彼此的传输。在公共或非对称加密术中，有两把钥匙并存：公钥和密钥。某人或某机构把他们的密钥保密，只公布他们的公钥；使用密钥编码的数据只能用公钥才 能解码。

要设置你的安全服务器，你将会使用工具来创建公钥和密钥对。在多数情况下，你会向某 CA 发送证书请求（包括你的公钥）、你的公司身份的证据、以及付款。CA 将会校验你的证书请求和身份，然后把你的安全万维网证书寄回给你。

另外，你也可以创建你自己的自签证书。然而请注意，自签证书不应该被用在多数商业环境中。自签证书不会被用户的浏览器自动接受。

在你有了自签的证书或来自 CA 的证书后，你需要把它安装在你的安全服务器上。

3.12.4 使用已存钥匙和证书

如果你已有现存的钥匙和证书（例如，如果你要安装安全服务器来替换另一家公司的安全服务器产品），你可能将能够在安全服务器中使用你现存的钥匙和证书。在下面这两种情况下，你将无法使用现存的钥匙和证书：

- 如果你改变了你的 IP 地址和域名 — 证书是向特定 IP 地址和域名对颁发的。如果你改变了域名或 IP 地址，你需要申请一份新证书。

- 如果你有一份来自 VeriSign 的证书，但想改变服务器软件。如果你已有一份由于其它原因而获得的 VeriSign 证书，你可能会考虑在你的新安全服务器中使用现有的 VeriSign 证书，然而，你将不会被允许使用它。这是因为 VeriSign 依据特定服务器软件和 IP 地址/域名组合来颁发证书。

如果你改变了以上任一参数（譬如，从前你使用了另一个安全服务器产品，现在你想使用这个安全服务器），你为从前的配置所获取的 VeriSign 证书将无法在新配置中使用。你必须获取一份新证书。

当你获得了新的钥匙对和证书以后，把你的钥匙文件转移到 /etc/httpd/conf/ssl.key/server.key 中，将证书文件转移到 /etc/httpd/conf/ssl.crt/server.crt。然后就可以测试证书，测试方法稍后会有介绍。

最后，使用 service httpd restart 来重新启动服务器以便激活安全服务器。

3.12.5 证书类型

在使用安全服务器之前，你需要生成你自己的钥匙并获取正确识别你的服务器的证书。

证书有两种类型：

- 一种是从某 CA 处购买的由 CA 签名的证书。由 CA 签名的证书为你的服务器提供两项重要能力：

浏览器（通常）会自动识别证书，并且不必提示用户就能够允许开通安全连接

当某 CA 颁发了签名的证书，他们是在向浏览器担保提供网页的机构的身份。

如果你的安全服务器被广大公众所访问，你的安全服务器需要有 CA 签名的证书，因此访问你的网站的用户可以信任该网站的确是他自己所声明的。在签发证书前，CA 校验申请证书的机构也必须确认网站的声明的真实与否。

多数支持 SSL 的万维网浏览器有一个它们会自动接受证书的 CA 列表。如果浏览器遇到一份来自列表之外的授权 CA 的证书，浏览器会询问用户是否要接受连接。

- 另一种证书类型是自签型证书，也就是证书是由服务者本身所签发的，但是自签证书将不会提供和 CA 签发的证书相同的功能。自签证书将不会被用户的浏览器自动识别，而且它将不会担保提供网站的机构的身份。

因此，如果你的服务器是要应用于商业或者是生产环境下的，你应该使用 CA 签发的证书。从 CA 获取证书的手续非常简单。下面是对其步骤的简单描述：

创建加密的公钥和密钥对。

根据公钥创建证书请求。证书请求包括服务器和它所属公司的信息。

向某 CA 发送证书请求，以及证明你的身份的文档。 当你选定了一个

CA 后，你需要遵循他们提供的说明来获取证书。

当 CA 对你的身份的真实性核对无误后，他们就会给你寄发一份数字证书。

在你的安全服务器上安装该证书，然后开始处理安全事务。

不论你是从 CA 处获取证书，还是使用自签的证书，第一个步骤都是生成钥匙。

3.12.6 生成钥匙

首先，进入到 /etc/httpd/conf 目录中，使用下面的命令删除在安装中生成的模拟的钥匙和证书：

```
rm ssl.key/server.key

rm ssl.crt/server.crt
```

然后，你需要生成你自己的随机钥匙。改换到 /usr/share/ssl/certs 目录中，键入命令 make genkey，你的系统会显示类似下面的信息：

```
umask 77 ; \

/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key\

/server.key

Generating RSA private key, 1024 bit long modulus

.......++++++

................................................................

++++++

e is 65537 (0x10001)

Enter PEM pass phrase:
```

此时，需要你输入口令，每次启动安全服务器的时候都需要这个口令进行验证，因此请确保这个口令的安全性。口令的长度至少需要包含 8 个字符，同时口令是区分大小写的。

当成功输入口令后，在目录/etc/httpd/conf/ssl.key/下会生成 server.key 文件。这个就是你的钥匙文件，请妥善保管。

如果在启动安全服务器的时候不想输入口令的话，可以使用下面的方法来生成钥匙文件，首先使用 openssl 产生钥匙：

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

然后使用命令 chmod 来确保该钥匙文件的权限是正确的。

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

使用以上的命令生成钥匙文件以后，则再次启动安全服务器不会提示输入口令。但是需要提醒的一点是，不进行口令检验是一种具有潜在风险的操作，因此，商业用户还是应该采用输入口令的方式启动安全服务器。

生成的钥匙文件 server.key 应该被根用户所拥有，不应该被其它用户访问，并且应该为该文件备份，将备份副本存放在安全的地方。钥匙文件需要备份的原因是，如果你在使用钥匙创建了证书请求后丢失了 server.key 文件，你的证书就不会再生效，而 CA 对此也爱莫能助。你只能再申请（并购买）一份新证书。

3.12.7 生成发送给 CA 的证书请求

一旦你创建了钥匙，下一步就是生成证书请求，你需要把该请求发送给选中的 CA。请确定你位于 /usr/share/ssl/certs 目录，并键入下面的命令:make certreq。这时系统会显示下列输出，然后还会请你输入口令句 （除非你禁用了口令选项）。

```
umask 77 ; \

/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key

-out /etc/httpd/conf/ssl.csr/server.csr

Using configuration from /usr/share/ssl/openssl.cnf

Enter PEM pass phrase:
```

键入你在生成钥匙时选择的口令。你的系统将会显示一些指示，然后向你

询问一系列问题。你的输入会被包括在证书请求中。所显示的输出和示例回答，看起来和下面相似：

```
You are about to be asked to enter information that will be \
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name\
or a DN.
There are quite a few fields but you can leave some blank \
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:CN
State or Province Name (full name) [Berkshire]:BeiJing
Locality Name (eg, city) [Newbury]:BeiJing
Organization Name (eg, company) [My Company Ltd]:Turbolinux
Organizational Unit Name (eg, section) []:RD
Common Name (your name or server's hostname) []:turbolinux.com.cn
Email Address []:admin@turbolinux.com.cn
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

默认回答紧随在每项要求后面的括号内 ([])。其填入的内容依次为：

- 国家代码
- 所在省份

- 所在城市
- 公司名称
- 所在部门
- 主机名称：请输入安全服务器的有效 DNS 名称。
- 邮件地址：通常是网络管理员的邮件地址。

不要输入最后两项，这两个附加属性是不必要的。同时在输入的过程中，请避免使用诸如@、#、&、！这样的特殊字符，因此，如果你的公司名称包含 &，把它拼写为“and”。

信息输入完毕后，一个叫做 /etc/httpd/conf/ssl.csr/server.csr 的文件就会被创建。该文件是你的证书请求，可以随时寄发给你的 CA。

在你选定了 CA 后，按照他们在网站提供的说明行事。这些说明会告诉你如何发送证书请求，你还需要哪些文档以及付款信息。

在你满足了 CA 的要求后，他们就会给你寄发证书（通常通过电子邮件）。将它们寄发的证书保存为（或剪贴为） /etc/httpd/conf/ssl.crt/server.crt。请确定给该文件保留一份备份。

3.12.8 创建自签的证书

你可以创建自签的证书。请注意，自签的证书将不会提供由 CA 签发的证书所提供的安全担保。如果你想制作自签的证书，你首先需要按照前面章节所述的过程来创建随机钥匙。一旦创建了钥匙，请确定你位于 /usr/share/ssl/certs 目录中，再键入下面的命令：

```
make testcert
```

你将会看到以下输出，你会被提示输入口令句（除非你生成了无口令的钥匙）：

```
umask 77 ; \

/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key

-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
```

```
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

输入口令句后（如果你创建了无口令的钥匙则没有提示），你会被要求输入更多信息。计算机的输出以及一组示例输入与以下的显示相仿（你需要为你的主机和机构提供正确的信息）：

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:CN
State or Province Name (full name) [Berkshire]:BeiJing
Locality Name (eg, city) [Newbury]:BeiJing
Organization Name (eg, company) [My Company Ltd]:turbolinux
Organizational Unit Name (eg, section) []:RD
Common Name (your name or server's hostname) []:tt@emp.com.cn
Email Address []:myemail@example.com
```

提供了正确信息后，自签的证书就会在 /etc/httpd/conf/ssl.crt/server.crt 中被创建。生成证书后，你需要使用以下命令来重新启动安全服务器：

```
/sbin/service httpd restart
```

3.12.9 测试自签的证书

要测试默认安装的测试证书、CA 签发的证书、以及自签的证书，将你的主页替换成为具有 https://头的主页名称。如果你使用的是由知名 CA 签发的证书，你的浏览器可能会自动接受该证书（不必提示你输入）并创建安全连接。你的浏览器不会自动识别测试或自签的证书，因为这些证书不是由 CA 签发的。如果你没有使用来自 CA 的证书，请遵循浏览器的指示来接受证书。你的浏览器接受了证书后，你的安全服务器就会显示默认的主页。

3.12.10 访问服务器

要访问你的安全服务器，使用和以下相似的 URL：

https://server.example.com

安全万维网通讯的标准端口是端口 443。非安全万维网通讯的标准端口是端口 80。安全服务器默认配置对这两个端口都监听。因此，你不必在 URL 中指定端口号码（端口号码会被假定）。 然而，如果你配置了你的服务器监听非标准的端口（除 80 和 443 之外的），你必须在每个 URL 中指定旨在非标准端口上连接服务器的端口号码。

例如，你可能给你的服务器做了相应配置，因此你在端口 15000 上运行一个非安全的虚拟主机。任何旨在连接该虚拟主机的 URL 都必须在 URL 中指定端口号码。下面的 URL 例子会试图连接在端口 15000 监听的非安全万维网服务器

http://server.example.com:15000

3.13 验证配置

当用户登录入 Turbolinux 系统，其用户名和口令的组合必须被校验或验证（authenticated）以判定他是否为有效的活跃用户。有时，用于校验用户的信息位于本地系统；有时，系统把验证推延给远程系统上的用户数据库。

证配置工具提供了配置 NIS、LDAP、和 Hesiod 来检索用户信息，以及把 LDAP、Kerberos、和 SMB 配置成验证协议的图形化界面。

从桌面上启动图形化版本的 验证配置工具，选择面板上的主菜单选择系统设置中的验证项。也可以在 shell 提示下键入 authconfig 命令进行手工配置。

3.13.1 用户信息

用户信息标签上有几个选项。要启用选项，点击它旁边的空白复选框。要禁用选项，点击它旁边的复选框来清空它。如果确定上述的改变，则点击确定保存所进行的配置。



图 3-35 验证配置—用户信息

页面上有如下的配置区域：

- 缓存用户信息：选择该选项来启用名称服务缓存守护进程（nscd)，并配置它在引导时启动。你必须安装了 nscd 软件包才能使这个选项奏效。

- 启用 NIS 支持：选择该选项来把系统配置成连接 NIS 服务器来验证用户和口令的 NIS 客户。点击配置 NIS 按钮来指定 NIS 域和 NIS 服务器。

如果 NIS 服务器没有被指定，守护进程会试图通过广播来寻找它。你必须安装了 ypbind 软件包才能使这个选项奏效。如果启用了 NIS 支持，portmap 和 ypbind 服务会被启动，它们也会在引导时被启用。

- 启用 LDAP 支持：选择这个选项来配置系统来通过 LDAP 检索用户信息。点击"配置 LDAP"按钮来指定"LDAP 搜索基准 DN"和"LDAP 服务器"。如果"使用 TLS 来加密连接"被选择，传输层安全就会被用来加密发送给 LDAP 服务器的口令。你必须安装 openldap-clients 软件包才能使这个选项奏效。

- 启用 Hesiod 支持：选择这个选项来配置系统来从远程 Hesiod 数据库中检索信息，包括用户信息。你必须要安装 hesiod 软件包。

- 启用 Winbind 支持：选择这个选项使系统可以连接到 Windows Active Directory 或者 Windows domain controller。

3.13.2 验证

验证标签允许你配置网络验证方法。要启用选项，点击它旁边的空白复选箱。要禁用选项，点击它旁边的复选箱来清空它。

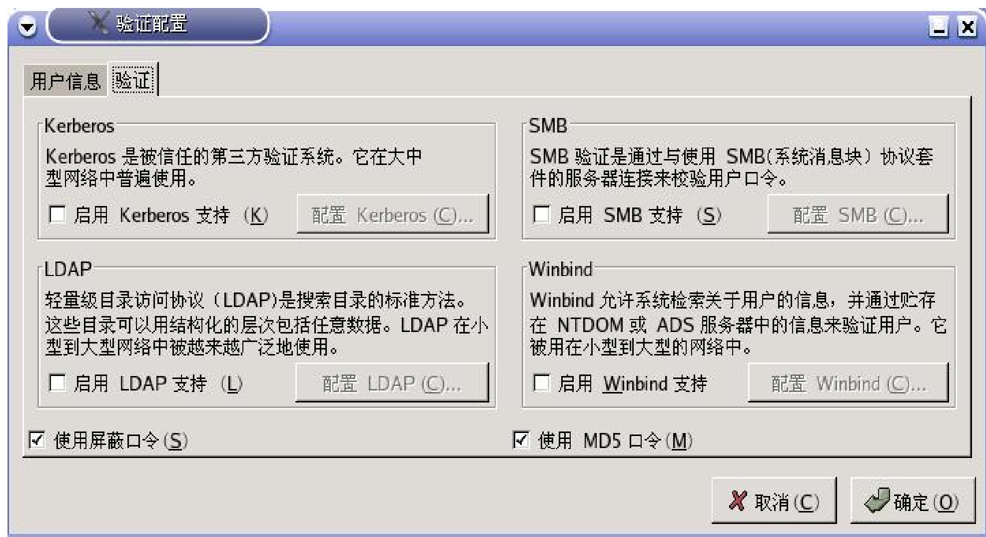


图 3-36 验证配置－验证

标签中有以下的配置区域：

- 使用屏蔽口令：选择这个选项来在 /etc/shadow 文件中而不是 /etc/passwd 文件把口令贮存为屏蔽口令格式。屏蔽口令在安装中被默认启用，它也是我们极力推荐你用来增加系统安全性的措施。你必须安装了 shadow-utils 软件包才能使这个选项奏效。

- 使用 MD5 口令：选择这个选项来启用 MD5 口令。它会允许长达 256 个字符的口令而不同是通常的少于八个字符的口令。该选择在安装中被默认选择，它也是我们极力推荐你用来增加系统安全性的措施。

- 启用 LDAP 支持：选择这个选项来让标准的启用 PAM 的应用程序使用 LDAP 来验证。点击“配置 LDAP”按钮可以指定三种信息。使用 TLS 来加密连接，LDAP 搜索基准 DN，LDAP 服务器。你必须安装了 openldap-clients 软件包才能使这个选项奏效。

- 启用 Kerberos 支持： 选择这个选项来启用 Kerberos 验证。点击“配置 Kerberos”按钮来配置，可以进行三种配置。

领域：配置 Kerberos 服务器的领域。领域是使用 Kerberos 的网络，由一个或多个 KDC，以及大量客户组成。

KDC：定义密钥分发中心（KDC）。它是分发 Kerberos 门票的机器。

管理服务器：指定运行 kadmind 的管理服务器。

你必须安装 krb5-libs 和 krb5-workstation 软件包才能使这个选项奏效。

- 启用 SMB 支持： 该选项配置 PAM 使用 SMB 服务器来验证用户。点击“配置 SMB”按钮来指定两项配置。

工作组：指定要使用的 SMB 工作组。

域控制器：指定要使用的 SMB 域控制器。

3.14 控制台访问

当普通用户（非根用户）在本地登录到计算机上，他们被授予两类特殊权

限：

- 可以运行某些通常无法运行的程序
- 可以访问某些通常无法访问的文件（通常是用来访问磁盘、光盘等的特殊设备文件）

由于单个计算机有多个控制台，多位用户可以在同一时间内在计算机上本地登录，其中之一必定在访问这些文件的角逐中“获胜”。第一个在控制台登录的用户完全拥有那些文件。一旦第一个用户注销，下一个登录的用户就会拥有这些文件。

与之相反，每个在控制台登录的用户都被允许运行通常只限于根用户的程序来完成任务。如果 X 在运行，这些行动可以被包括在图形化用户界面的菜单内。在该发行版本中，可从控制台访问的程序包括 halt、poweroff、和 reboot。

3.14.1 禁用通过 Ctrl-Alt-Del 关机

按照默认设置，/etc/inittab 文件指定你的系统可在控制台使用 [Ctrl]-[Alt]-[Del] 键组合来关闭并重启系统。如果你想完全禁用这项能力，你需要把 /etc/inittab 文件中下面一行变成注释，方法是在句前加一个井号（#）：

```
ca::ctrlaltdel:/sbin/shutdown-t3-rnow
```

另外，你可能只是想授予个别非根用户从控制台使用 [Ctrl]-[Alt]-[Del] 来重启系统的权利。你可以通过下面的步骤来把该特权仅限定给某些用户使用：

在上面显示的 /etc/inittab 的那一行中添加 -a 选项，如下所示：

```
ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
```

-a 标志通知 shutdown 命令去寻找 /etc/shutdown.allow 文件，我们在下一步骤中将会创建该文件。

在 /etc 目录中创建一个叫做 shutdown.allow 的文件。shutdown.allow 文

件应该列出允许使用 [Ctrl]-[Alt]-[Del] 来关闭系统的用户名。/etc/shutdown.allow 文件使用列表格式，每行列出一名用户，如下所示：

```
stephen

jack

sophie
```

根据以上 shutdown.allow 文件的例子，stephen、jack、和 sophie 被允许使用 [Ctrl]-[Alt]-[Del] 来从控制台关闭系统。当这个键组合被使用时，/etc/inittab 中的 shutdown -a 就会查看 /etc/shutdown.allow 中列出的用户（或根用户）是否在虚拟控制台上登录了。如果登录者是其中之一，系统关闭就会继续；否则，系统控制台上就会显示出错误消息。

3.14.2 禁止执行控制台程序

为禁止用户执行控制台程序，请使用超级用户执行如下命令：

```
rm -f /etc/security/console.apps/*
```

在控制台没有被保护的环境下（BIOS 和引导装载程序的口令没有被设置；[Ctrl]-[Alt]-[Delete] 键组合没有被禁用；电源和重设开关没有被禁用等等），你可能不想允许任何用户在控制台上运行这些默认可以从控制台上使用的命令：poweroff、halt、和 reboot。

禁止这些操作，可以使用 root 用户执行如下命令：

```
rm -f /etc/security/console.apps/poweroff

rm -f /etc/security/console.apps/halt

rm -f /etc/security/console.apps/reboot
```

3.14.3 定义控制台

pam_console.so 模块使用 /etc/security/console.perms 文件来判定系统控制台上用户的权限。该文件的语法非常灵活；你可以编辑该文件以便 不再

应用这些指示。然而，默认文件中有一行看起来如下：

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

当用户登录后，他们会被连接到某种有名称的控制台，要么是名称类似 :0 或 mymachine.example.com:1.0 的 X 服务器，要么是类似 /dev/ttyS0 或 /dev/pts/2 的设备。默认设置中，本地虚拟控制台和本地 X 服务器被定义为本地，但是如果你想把和你相邻的位于端口 /dev/ttyS1 上的串线终端也当作本地，你可以把上面一行改为：

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

3.14.4 使文件可从控制台访问

/etc/security/console.perms 文件中的某段包含以下几行：

```
<floppy>=/dev/fd[0-1]*\

/dev/floppy/*/mnt/floppy*

<sound>=/dev/dsp*/dev/audio*/dev/midi*\

/dev/mixer*/dev/sequencer\

/dev/sound/*/dev/beep

<cdrom>=/dev/cdrom*/dev/cdroms/*/dev/cdwriter*/mnt/cdrom*
```

如果有必要，你可以在这段里加入你自己编写的句子。请确定你添加的句中所指代的是正确的设备。譬如，你可以添加以下这一行：

```
 <scanner>=/dev/scanner/dev/usb/scanner*
```

（当然，请确定 /dev/scanner 的确是你的扫描仪设备，而不是你的硬盘驱动器。）

这是第一步。第二步是定义如何处置那些文件。在 /etc/security/console.perms 文件的最后一段寻找与以下类似的句子：

```
<console>0660<floppy>0660root.floppy

<console>0600<sound>0640root
```

```
<console>0600<cdrom>0600root.disk
```

然后，添加和以下类似的一行：

```
<console> 0600 <scanner> 0600 root
```

当你在控制台登录后，你就会被给予 /dev/scanner 设备的所有权，其权限是 0600（仅可被你读写）。当你注销后，该设备就会被根用户所有，权限依旧是 0600（现在将只能被根用户读写）。

3.14.5 为其它应用程序启用控制台访问

如果你想使其它应用程序能被控制台用户访问，你要采取的步骤就会多一些。

首先，只有驻留在 /sbin 或 /usr/sbin 中的应用程序才能在控制台上访问，因此你想运行的程序也必须被保存在那两个目录中。满足了上面的条件后，执行下面的步骤：

- 创建一个从你的应用程序（如以下例子中的 foo）到 /usr/bin/consolehelper 的链接：

```
cd /usr/bin

ln -s consolehelper foo
```

- 创建文件 /etc/security/console.apps/foo：

```
touch /etc/security/console.apps/foo
```

- 在 /etc/pam.d/ 目录中为 foo 服务创建一个 PAM 配置文件。做到它的简单方法是使用 halt 服务的 PAM 配置文件的副本，如果你想改变行为的话，修改该文件：

```
cp /etc/pam.d/halt /etc/pam.d/foo
```

现在，当你运行 /usr/bin/foo 时，它就会 调用 consolehelper，该命令会借助 /usr/sbin/userhelper 来验证用户。要验证用户， consolehelper 会询问用户的口令（若 /etc/pam.d/foo 是 /etc/pam.d/halt 文件的副本的话，否则，它 会仅执行在 /etc/pam.d/foo 中的命令），然后使用根权限来运行

/usr/sbin/foo。

在 PAM 配置文件中，应用程序可以被配置使用 pam_timestamp 模块来记住（缓存）一次成功的尝试。当应用程序被启动并提供了正确的验证后（根口令），一个时间戳文件就会被创建。按照默认设置，成功验证会被缓存五分钟。在这段时期内，在同一会话中运行的其它配置使用 pam_timestamp 的应用程序会自动为该用户验证 — 用户不必再输入根口令。

该模块被包括在 pam 软件包中。要启用这项功能，etc/pam.d/ 中的 PAM 配置文件必须包括以下几行：

```
authsufficient/lib/security/pam_timestamp.so

sessionoptional/lib/security/pam_timestamp.so
```

第一个以 auth 开头的行应该在任何 auth sufficient 行之后，以 session 开头的行应该在所有 session optional 行之后。

如果配置使用 pam_timestamp 的从面板上的“主菜单”按钮启动的应用程序被成功地验证，图标就会显示在面板的通知区域（若你运行的是 GNOME 桌面环境）。验证过期后（默认为五分钟），该图标就会消失。

用户可以通过点击图标并选择忘记验证选项来忘记缓存验证。

3.14.6 floppy 组群

如果由于某种原因，控制台访问对你不适用，你需要给非根用户提供到系统软盘驱动器的访问，这可以通过使用 floppy 组群来达到。使用你选定的工具把用户添加到 floppy 组群就可以了。这里向你提供了一个如何使用 gpasswd 来把用户 fred 添加到 floppy 组群的例子：

```
[root@bigdog root]# gpasswd -a fred floppy

Adding user fred to group floppy

[root@bigdog root]#
```

现在，用户 fred 就可以通过控制台访问系统的软盘驱动器了。

3.15 配置日期和时间

时间和日期属性工具允许用户改变系统日期和时间；配置系统使用的时区；以及设置网络时间协议（NTP）守护进程来与时间服务器的系统时钟同步。

你必须运行 X 窗口系统并具备根特权。要从桌面上启动这个程序，点击“主菜单 –> 系统设置 –> 日期 & 时间”。

3.15.1 时间和日期属性

如图 3-37 所示，所出现的第一个带标签的窗口被用来配置系统日期、时间和 NTP 守护进程（ntpd）。

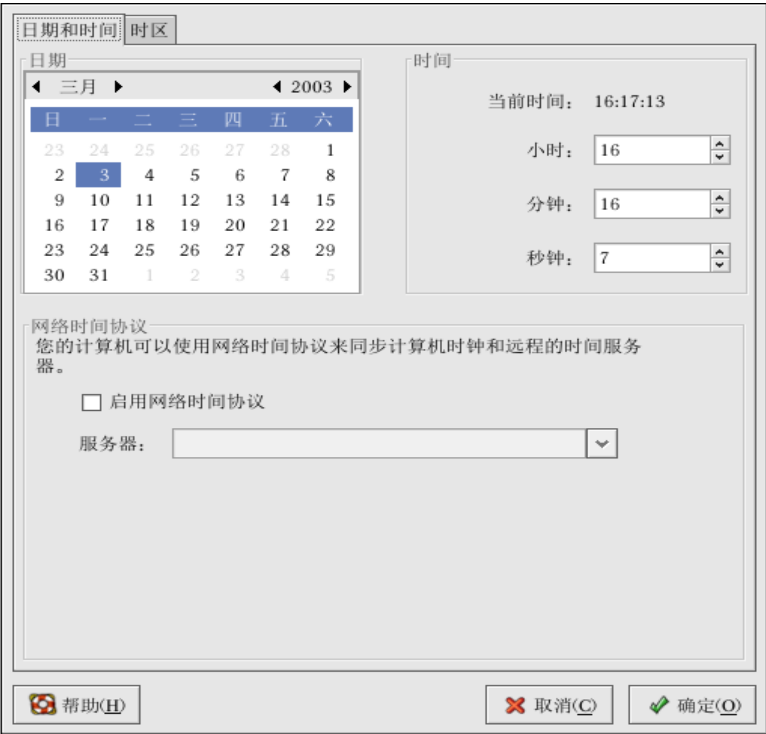


图 3-37 时间和日期属性

要改变日期，使用箭头左右移动月份来改变月份；使用箭头左右移动年份来改变年份，然后点击星期中的日期来改变星期中的日期。在点击“确定”按钮之前，这些改变不会生效。

要改变时间，使用上下箭头按钮，它们在“时间”部分中的“小时”、“分钟”、和“秒钟”旁边。在你点击“确定”按钮之前，这些改变不会生效。

网络时间协议（NTP）守护进程使用远程时间服务器或时间源（如卫星）来同步系统时钟。该程序允许你配置 NTP 守护进程来与远程服务器同步你的系统时钟。要启用这项功能，点击“启用网络时间协议”按钮。这会启用“服务器”拉下菜单。你可以选择预定义的服务器中的一个，或键入拉下菜单中的一个服务器名。在你点击“确定”之前，你的系统不会开始与 NTP 服务器的同步。在你点击“确定”之后，配置就会被存盘，NTP 守护进程就会被启动（或重新启动，如果它已在运行）。

点击“确定”按钮会应用你对日期和时间所做的改变、NTP 守护进程设置、以及时区设置，然后退出程序。

3.15.2 时区配置

要配置系统时区，点击“时区”标签。时区可以通过互动地图来改变，也可以从地图下面的列表中选择想要的时区。要使用地图，点击代表你想要时区的城市，一个红色的“X”会出现，地图下面的列表中的时区选择也会相应改变。点击“确定”来应用改变并退出程序。



图 3-38 时区属性

如果你的系统时钟被设为使用 UTC，选择“系统时钟使用 UTC”选项。UTC 代表通用时区，又称格林威治标准时间（GMT）。其它时区是通过从 UTC 时间中加减而得出的。

3.16 键盘配置

安装程序允许用户为他们的系统配置键盘布局。要在安装后配置不同的键盘布局，请使用键盘配置工具。

要启动键盘配置工具，选择面板上的“主菜单 —> 系统设置 —> 键盘”，或在 shell 提示下键入 system-config-keyboard 命令。

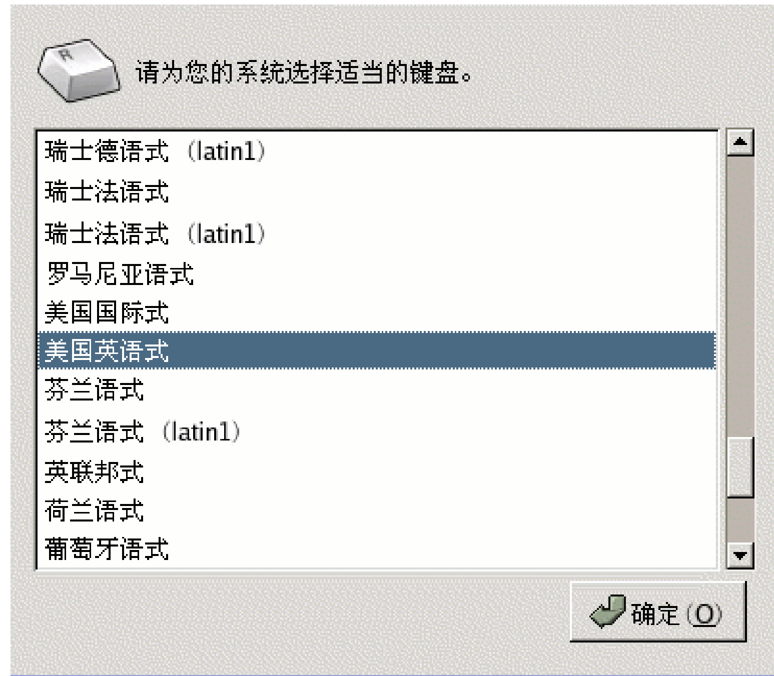


图 3-39 键盘配置工具

从列表中选择键盘布局（如“美国英语式）)，然后点击“确定”。要使改变立即生效，你应该退出图形化桌面会话后再重新登录。

3.17 鼠标配置

安装程序允许用户选择连接到系统上的鼠标类型。要为系统配置不同的鼠标，请使用鼠标配置工具。

要启动鼠标配置工具，点击面板上的“主菜单 —> 系统设置 —> 鼠标”，或者在 shell 提示（如 XTerm 或 GNOME 终端）下键入 system-config-mouse 命令。如果你没有运行 X 窗口系统，所运行的就会是该工具的文本模式版本。

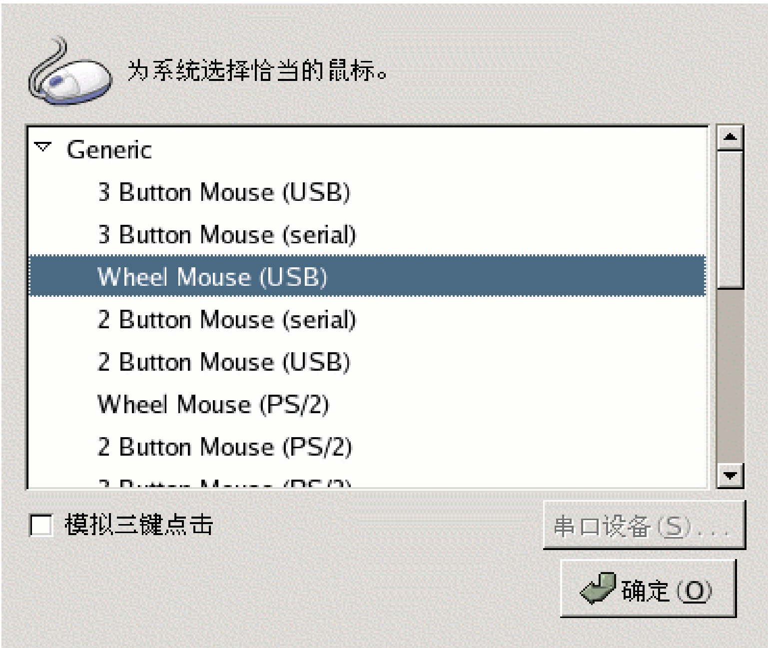
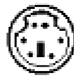


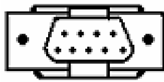
图 3-40 选择鼠标

为你的系统选择新的鼠标类型。如果你找不到确切的匹配，选择你肯定会与系统兼容的鼠标类型。

内建的指示设备，如便携电脑上的触摸板，通常是 PS/2 兼容的。

所有的鼠标类型都在括号内注明了“PS/2”、“串口”或“USB”。它们指定鼠标的端口。

PS/2 鼠标的端口看起来象是：。

串口鼠标的端口看起来象是：。

USB 鼠标的端口看起来象是：。

如果某种特定的鼠标没有被列出，请根据你的鼠标的键数和接口，选择“通用”项目中的一个。

滑轮鼠标上的滑轮可以被当作鼠标中键使用，可以用来进行剪切、粘贴文本等鼠标中键功能。如果鼠标只有两键，选择“模拟三键点击”来把两键鼠标当作三键鼠标使用。当你启用了这个选项后，同时点击鼠标的两键就会模拟鼠标中键点击。

如果选择了串口鼠标，点击“串口设备”按钮来为鼠标配置正确的串口设备号码，如 /dev/ttyS0。

点击“确定”来保存新的鼠标类型。你的选择被写入 /etc/sysconfig/mouse 文件，控制台的鼠标服务以及 gpm 被重新启动。这些改变也被写入 X 窗口系统的配置文件 /etc/X11/XF86Config 中；不过，鼠标类型改变没有被自动应用到当前的 X 会话。要启用新的鼠标类型，退出图形化桌面后再重新登录。

3.18 X 窗口系统配置

在安装中，系统的显示器、视频卡和显示设置都被配置了。要改变这些设置，请使用 X 配置工具。

要启动 X 配置工具，选择面板上的“主菜单 —> 系统设置 —> 更多系统设置 —> 显示”，或在 shell 提示（如 XTerm 或 GNOME 终端）下键入 system-config-display 命令。如果 X 窗口系统没在运行，一个小型的 X 会被启动来运行这个程序。

改变了这些设置后，退出图形化桌面后再重新登录来启用所做改变。

3.18.1 显示设置

“显示”活页标签会允许用户改变分辨率（resolution）和色彩深度（color depth）。显示器的显示包含叫做像素（pixels）的小点。一次显示的像素数量叫做分辨率。例如：分辨率 1024x768 意味着使用了 1024 个水平像素，768 个垂直像素。分辨率数字越高，显示器在一次显示中所显示的图像就越多。例如：分辨率越高，桌面图标就显得越小，填满整个桌面所需的图标就越多。

显示的色彩深度决定可能被显示的颜色数量。色彩深度越大，颜色的对比度就越强烈。



图 3-41 显示设置

3.18.2 高级设置

当程序被启动时，它会探测显示器和视频卡。如果硬件被正确探测了，这

些信息就会被显示在“高级”活页标签中。如图 3-42 所示。



图 3-42 高级设置

要改变显示器类型或它的设置，点击相应的“配置”按钮。要改变视频卡类型或它的设置，点击设置旁边的“配置”按钮。

3.19 用户和组群配置

用户管理器允许你查看、修改、添加和删除本地用户和组群。

要使用用户管理器，你必须运行 X 窗口系统，具备根特权，并且安装了 system-config-users RPM 软件包。要从桌面启动用户管理器，点击面板上的“主菜单 —> 系统设置 —> 用户和组群”，或在 shell 提示（如 XTerm 或 GNOME 终端）下键入 system-config-users 命令。

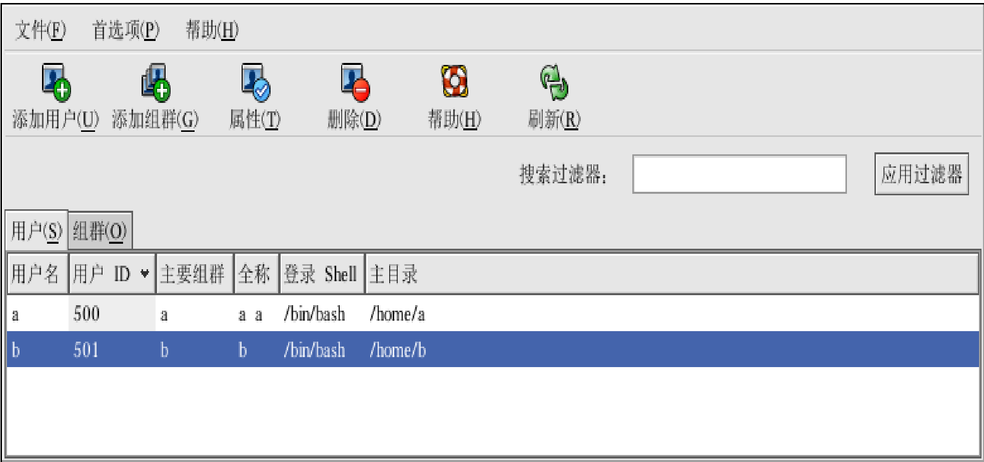


图 3-43 用户管理器

- 要查看包括系统内本地用户的列表，点击“用户”标签。要查看包括系统内本地组群的列表，点击“组群”标签。

- 要寻找指定的用户或组群，在“搜索过滤器”字段内键入名称的前几个字符。按 [Enter] 键或点击“应用过滤器”按钮。被过滤的列表就会被显示。

- 要给用户和组群排序，点击列名。用户或组群就会按照该列的信息被排序。

GTES10 把 500 以下的用户 ID 保留给系统用户。用户管理器默认不显示系统用户。要查看包括系统用户在内的所有用户，从“首选项”拉下菜单中取消选择“过滤系统用户和组群”。

3.19.1 添加新用户

要添加新用户，点击“添加用户”按钮。一个如图 3-44 所示的窗口就会出现。在适当的字段内键入新用户的用户名和完整姓名。在“口令”和“确认口令”字段内键入口令。口令必须至少包含六个字符。

选择一个登录 shell。如果你不能确定应该选择哪一个 shell，就请接受默

认的 /bin/bash。默认的主目录是 /home/用户名/。你可以改变为用户创建的主目录，或者通过取消选择“创建主目录”来不为用户创建主目录。

如果你选择要创建主目录，默认的配置文件就会从 /etc/skel/ 目录中复制到新的主目录中。

GTES10 使用用户私人组群（user private group，UPG）方案。UPG 方案并不添加或改变 UNIX 处理组群的标准方法；它只不过提供了一个新约定。按照默认设置，每当你创建一个新用户的时候，一个与用户名相同的独特组群就会被创建。如果你不想创建这个组群，取消选择“为该用户创建私人组群”。

要为用户指定用户 ID，选择“手工指定用户 ID”。如果这个选项没有被选，从号码 500 开始后的下一个可用用户 ID 就会被分派给新用户。GTES10 把低于 500 的用户 ID 保留给系统用户。

点击“确定”来创建该用户。

用户名：

全称：

口令：

确认口令：

登录 Shell： /bin/bash

创建主目录

主目录： /home/

为该用户创建私人组群

手工指定用户 ID

UID： 500

取消(C) 确定(O)

图 3-44 创建新用户

要把用户加入到更多的用户组群中，点击“用户”标签，选择该用户，然后点击“属性”。在“用户属性”窗口中，选择“组群”标签。选择你想让该用户加入的组群，以及用户的主要组群，然后点击“确定”。

3.19.2 修改用户属性

要查看某个现存用户的属性，点击“用户”标签，从用户列表中选择该用户，然后在按钮菜单中点击“属性（或者从拉下菜单中选择“文件”） －> 属性”）。一个类似图 3-45 的窗口就会出现。

图 3-45 用户属性

“用户属性”窗口被分隔成多个带标签的活页：

- 用户数据 — 显示在你添加用户时配置的基本用户信息。使用这个标签来改变用户的全称、口令、主目录或登录 shell。

- 账号信息 — 如果你想让账号到达某一固定日期时过期，选择“启用账号过期”。在提供的字段内输入日期。 选择“用户账号已被锁”来锁住用户账号，从而使用户无法在系统登录。

- 口令信息 — 这个标签显示了用户口令最后一次被改变的日期。要强制用户在一定天数之后改变口令，选择“启用口令过期”。你还可以设置用户改变口令之前必须要经过的天数，用户被提醒去改变口令之前要经过的天数，以及账号变为不活跃之前要经过的天数。

- 组群 — 选择你想让用户加入的组群以及用户的主要组群。

3.19.3 添加新组群

要添加新用户组群，点击“添加组群”按钮。一个类似图 3-46 的窗口就会出现。键入新组群的名称来创建。要为新组群指定组群 ID，选择“手

工指定组群 ID”，然后选择 GID。GTES10 把低于 500 的组群 ID 保留给系统组群。

点击“确定”来创建组群。新组群就会出现在组群列表中。

图 3-46 创建新组群

3.19.4 修改组群属性

要查看某一现存组群的属性，从组群列表中选择该组群，然后在按钮菜单中点击“属性”（或选择拉下菜单“文件 —> 属性”）。一个类似图 3-47 的窗口就会出现。



图 3-47 组群属性

“组群用户”标签显示了哪些用户是组群的成员。选择其他用户来把他们加入到组群中，或取消选择用户来把他们从组群中移除。点击“确定”来修改该组群中的用户。

3.19.5 命令行配置

如果你更喜欢使用命令行工具，或者没有安装 X 窗口系统，请参考本节来配置用户和组群。

3.19.5.1 添加用户

要在系统上添加用户：

使用 useradd 命令来创建一个锁定的用户账号：

```
useradd <username>
```

使用 passwd 命令，通过指派口令和口令老化规则来给某账号开锁：

```
passwd <username>
```

useradd 的命令行选项在表 3-2 中被列出。

选项	描述
-c comment	用户的注释
-d home-dir	用来取代默认的 /home/username/ 主目录
-e date	禁用账号的日期，格式为：YYYY-MM-DD
-f days	口令过期后，账号被禁用前要经过的天数（若指定了 0，账号在口令过期后会被立刻禁用。若指定了-1，口令过期后，账号将不会被禁用）。
-g group-name	用户默认组群的组群名或组群号码（该组群在指定前必须存在）。
-G group-list	用户是其中成员的额外组群名或组群号码（默认以外的）的列表，用逗号分隔（组群在指定前必须存在）。
-m	若主目录不存在则创建它
-M	不要创建主目录
-n	不要为用户创建用户私人组群
-r	创建一个 UID 小于 500 的不带主目录的系统账号
-p password	使用 crypt 加密的口令
-s	用户的登录 shell，默认为 /bin/bash
-u uid	用户的 UID，它必须是独特的，且大于 499。

表 3-2. useradd 命令行选项

3.19.5.2 添加组群

要给系统添加组群，使用 groupadd 命令：

```
groupadd <group-name>
```

groupadd 的命令行选项在表 3-3 中被列出。

选项	描述
-g gid	组群的 GID，它必须是独特的，且大于 499
-r	创建小于 500 的系统组群
-f	若组群已存在，退出并显示错误（组群信息不会被改变）。若指定了 -g 和 -f 选项，但是组群已存在，-g 选项就会被忽略

表 3-3 groupadd 命令行选项

3.19.5.3 口令老化

为安全起见，要求用户定期改变他们的口令是明智之举。这可以在用户管理器的“口令信息”活页标签上添加或编辑用户时做到。

要从 shell 提示下为用户配置口令过期，使用 chage 命令，随后使用表 3-4 中的选项，以及用户的用户名。

选项	描述
-m days	指定用户必须改变口令所间隔的最少天数。如果值为 0,，口令就不会过期。
-M days	指定口令有效的最多天数。当该选项指定的天数加上 -d 选项指定的天数小于当前的日期，用户在使用该账号前就必须改变口令。
-d days	指定自从 1970 年 1 月 1 日起，口令被改变的天数。
-I days	指定口令过期后，账号被锁前不活跃的天数。如果值为 0，账号在口令过期后就不会被锁。

-E date	指定账号被锁的日期，日期格式为 YYYY-MM-DD。若不用日期，也可以使用自 1970 年 1 月 1 日后经过的天数。
-W days	指定口令过期前要警告用户的天数。

表 3-4 chage 命令行选项

如果系统管理员想让用户在首次登录时设置口令，用户的初始口令或空口令可以被设置为立即过期，从而强制用户在首次登录后立即改变它。

要强制用户在首次登录到控制台时配置口令，请遵循以下步骤。注意，若用户使用 SSH 协议来登录，这个过程就行不通。

- 锁住用户的口令 — 如果用户不存在，使用 useradd 命令来创建这个用户账号，但是不要给它任何口令，所以它仍旧被锁。

如果口令已经被启用，使用下面的命令来锁住它：

```
usermod -L username
```

- 强制即刻口令过期 — 键入下面的命令：

```
chage -d 0 username
```

该命令把口令最后一次改变的日期设置为 epoch（1970 年 1 月 1 日）。不管口令过期策略是否存在，这个值会强制口令立即过期。

- 给账号开锁 — 达到这一目的有两种常用方法。管理员可以指派一个初始口令或空口令。

要指派初始口令，遵循以下步骤：

- 使用 python 命令来启动命令行 python 解释器。它的显示如下：

```
Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
[ GCC 3.2.1 20021207 (GTES10 3 3.2.1-2) ] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

- 在提示下，键入以下命令（把 password 替换成要加密的口令，把 salt

替换成恰巧两个大写或小写字母、数字、点字符或斜线字符，譬如 + ab 或 + 12）：

```
import crypt; print crypt.crypt("password","salt")
```

其输出的加密口令类似于 12CsGd8FRcMSM。

- 键入 [Ctrl]-[D] 来退出 Python 解释器。
- 把加密口令的输出剪贴到以下命令中（不带前后的空格）：

```
usermod -p "encrypted-password" username
```

与其指派初始口令，你还可以使用以下命令来指派空口令：

```
usermod -p "" username
```

无论是哪一种情况，首次登录后，用户都会被提示输入新口令。

3.19.6 对进程的解释

下列步骤演示了在启用屏蔽口令的系统上使用 useradd juan 命令后的情形：

- 在 /etc/passwd 文件中新添了有关 juan 的一行。这一行的特点如下：

  它以用户名 juan 开头。

  口令字段有一个“x”，表示系统使用屏蔽口令。

  500 或 500 以上的 UID 被创建。

  500 或 500 以上的 GID 被创建。

  可选的 GECOS 信息被留为空白。

  juan 的主目录被设为 /home/juan/。

  默认的 shell 被设为 /bin/bash。

- 在 /etc/shadow 文件中新添了有关 juan 的一行。这一行的特点如下：

  它以用户名 juan 开头。

  出现在 /etc/shadow 文件中口令字段内的两个叹号（!!）会锁住账号。

口令被设置为永不过期。

- 在/etc/group 文件中新添了一行有关 juan 组群的信息。和用户名相同的组群叫做用户私人组群（user private group）。

在 /etc/group 文件中新添的这一行具有如下特点：

它以组群名 juan 开头。

口令字段有一个“x”，表示系统使用屏蔽口令。

GID 与列举 /etc/passwd 文件中用户 juan 行中的相同。

在 /etc/gshadow 文件中新添了有关 juan 组群的一行。这一行的特点如下：

它以组群名 juan 开头。

- 出现在 /etc/gshadow 文件中口令字段内的一个叹号(!)会锁住该组群。

所有其它字段均为空白。

- 用于用户 juan 的目录被创建在 /home/ 目录之下。该目录为用户 juan 和组群 juan 所有。它的读写和执行权限仅为用户 juan 所有。所有其它权限都被拒绝。

- /etc/skel/ 目录（包含默认用户设置）内的文件被复制到新建的 /home/juan/ 目录中。

这时候，系统上就存在了一个叫做 juan 的被锁的账号。要激活它，管理员必须使用 passwd 命令给账号指派一个口令，他还可以设置口令老化规则。

3.20 打印机配置

打印机配置工具允许用户配置打印机。该工具为维护打印机配置文件、打印假脱机目录、和打印过滤器提供协助。

GTES10 使用 CUPS 打印系统。如果系统是从以前的使用 CUPS 的 GTES10 版本升级而来的，升级过程会保留配置的队列。

使用打印机配置工具要求你具备根特权。要启动这个应用程序，选择面板上的“主菜单 —> 系统设置 —> 更多系统设置 —> 打印”，或键入 systen-config-printer 命令。该命令会根据它所执行的环境是图形化桌面环境还是基于文本的控制台来自动判定它应该以图形化还是文本形式来运行。

要强制打印机配置工具作为基于文本的程序运行，你还可以在 shell 提示下键入 system-config-printer-tui 这个命令。



图 3-48 打印机配置工具

你可以配置以下类型的打印队列：

- 本地连接 — 直接通过并行或 USB 端口连接到计算机上的打印机。
- 联网的 CUPS (IPP) — 能够通过 TCP/IP 网络和互联网打印协议（Internet Printing Protocol，又称 IPP）而被使用的打印机（例如，连接到网络上另一个运行 CUPS 的 GTES10 系统上的打印机）。
- 联网的 UNIX (LPD) — 连接到能够通过 TCP/IP 网络而被使用的其它 UNIX 系统上的打印机（例如，连接到网络上另一个运行 LPD 的 GTES10 系统的打印机）。
- 联网的 Windows (SMB) — 连接到通过 SMB 网络来共享打印机的其它系统上的打印机（例如，连接到 Microsoft Windows™ 机器上的打印机）。
- 联网的 Novell (NCP) — 连接到使用 Novell's NetWare 网络技术的其

它系统上的打印机。

- 联网的 JetDirect — 通过 HP JetDirect 直接连接到网络而不是计算机上的打印机。

点击“应用”按钮来保存你所做的改变并重新启动打印机守护进程。这些改变在守护进程被重新启动前不会被写入配置文件。此外，你也可以选择“行动 —> 行动”。

3.20.1 添加本地打印机

要添加本地打印机，如通过并行端口或 USB 端口连接到你的计算机上的打印机，点击打印机配置工具主窗口上的“新建”按钮。一个如图 3-49 所示的窗口就会出现。点击“前进”来继续。

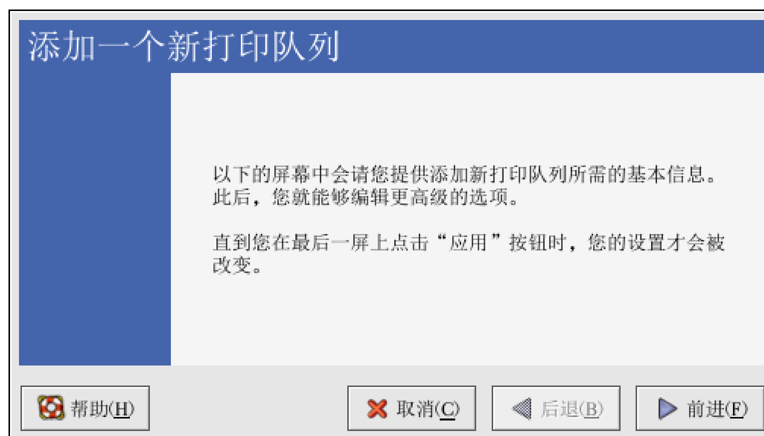


图 3-49 添加打印机

在如图 3-50 所示窗口中的“名称”文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入打印机的简短描述，其中可以包含空格。



图 3-50 选择队列名称

点击了“前进”后，如图 3-51 所示的窗口就会出现。从“选择队列类型”中选择“本地连接”，然后选择设备。这个设备通常是 /dev/lp0（并行打印机）或 /dev/usb/lp0（USB 打印机）。如果列表中没有设备，点击“重扫描设备”来重新扫描计算机或点击“定制设备”来手工指定它。点击“前进”来继续。

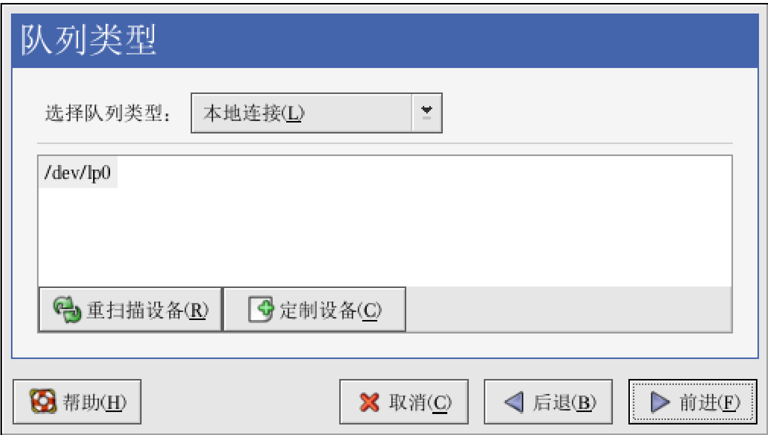


图 3-51 添加本地打印机

下一步是选择打印机类型。

3.20.2 添加一个 IPP 打印机

IPP 打印机是一种连接到运行 CUPS 的同一网络上的不同 Linux 系统上的打印机。按照默认配置，打印机配置工具浏览网络来寻找共享的 IPP 打印机。(该选项可以通过选择“行动 —> 共享)来改变。)任何通过 CUPS 的联网 IPP 打印机都会出现在“浏览队列”的主窗口中。

如果你在打印服务器上配置了防火墙，它必须能够在进入的 UDP 端口 631 上发送和接收连接。如果你在客户（发送打印请求的计算机）上配置了防火墙，它必须被允许在端口 631 上发送和接收连接。

如果你禁用了自动浏览功能，你仍可以通过打印机配置工具主窗口上的“新建”按钮来添加一个联网的 CUPS 打印机。它会显示一个如图 3-49 所示的窗口。点击“前进”来继续。

在如图 3-50 所示窗口中的“名称”文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入打印机的简短描述，其中可以包含空格。

点击了“前进”后，图 3-52 就会出现。从“选择队列类型”菜单中选择“联网的 CUPS (IPP) ”。

图 3-52 添加一个 IPP 打印机

用于以下选项的文本字段会出现：

- 服务器 — 打印机所连接的远程机器的主机名或 IP 地址。
- 路径 — 到远程机器上的打印队列的路径。

点击“前进”来继续。

下一步是选择打印机类型。

3.20.3 添加远程 UNIX (LPD)打印机

要添加远程 UNIX 打印机，如连接在同一网络上的不同 Linux 系统上的打印机，点击打印机配置工具主窗口上的“新建”按钮。如图 3-49 所示的窗口就会出现。点击“前进”来继续。

在如图 3-50 所示窗口中的“名称”文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入打印机的简短描述，其中可以包含空格。

从“选择队列类型”菜单上选择“联网的 UNIX (LPD) ”，然后点击“前进”。



图 3-53 添加远程 LPD 打印机

用于以下选项的文本字段会出现：

- 服务器 — 打印机所连接的远程机器的主机名或 IP 地址。
- 队列 — 远程打印机队列。默认打印机队列通常是 lp。

点击“前进”来继续。

3.20.4 添加 Samba (SMB)打印机

要添加使用 SMB 协议访问的打印机（如连接到 Microsoft Windows 系统上的打印机），点击打印机配置工具主窗口中的“新建”按钮。如图 3-49 所示的窗口就会出现。点击“前进”来继续。

在如图 3-50 所示窗口中的“名称”文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入打印机的简短描述，其中可以包含空格。

从“选择队列类型”菜单中选择“联网的 Windows (SMB) ”，然后点击“前进”。如果打印机连接的是 Microsoft Windows 系统，选择这个队列类型。

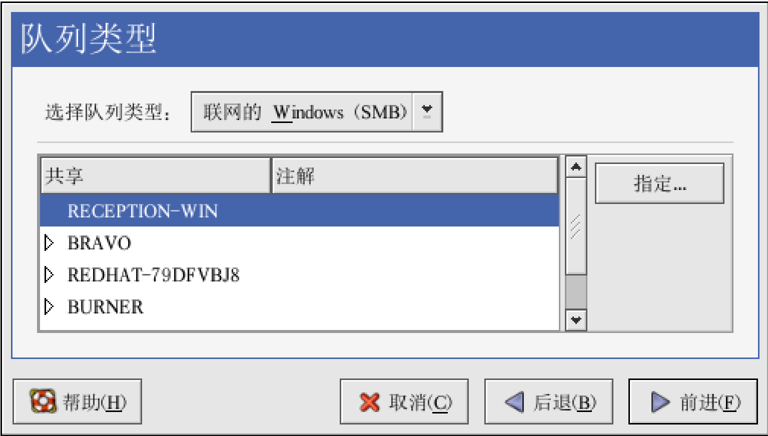


图 3-54 添加 SMB 打印机

如图 3-54 所示，SMB 共享被自动检测到并列出。点击每个共享名称旁的箭头来扩展列表。从扩展列表中选择一个打印机。

如果你在寻找的打印机没有在列表中出现，点击右侧的“指定”按钮。用于以下选项的文本字段会出现：

- 工作组 — 共享打印机的 Samba 工作组的名称。
- 服务器 — 共享打印机的服务器的名称。
- 共享 — 你想用来打印的共享打印机的名称。这个名称必须和远程 Windows 机器上定义的 Samba 打印机的名称相同。
- 用户名 — 你要访问打印机所必须登录使用的用户名称。用户在 Windows 系统上必须存在，并且必须有访问打印机的权限。默认的用户名典型为 guest（Windows 服务器）或 nobody（Samba 服务器）。
- 口令 — 在“用户名”字段中指定的用户的口令（若需要）。

点击“前进”来继续。然后，打印机配置工具会试图连接共享打印机。如果这个共享打印机需要用户名和口令，一个对话框会出现来提示你输入有效的共享打印机的用户名和口令。如果指定了正确的共享名称，你还可以在这里改变它。如果需要使用工作组名称来连接共享，它可以在这个对话框里指定。这个对话框和点击“指定”按钮后所显示的窗口相同。

下一步是选择打印机类型。

3.20.5 添加 Novell NetWare (NCP)打印机

要添加 Novell NetWare (NCP) 打印机，点击打印机配置工具主窗口上的“新建”按钮。如图 3-48 所示的窗口会出现。点击“前进”来继续。

在如图 3-50 所示窗口中的“名称”文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入打印机的简短描述，其中可以包含空格。

从“选择队列类型”菜单中选择“联网的 Novell (NCP) ”。

图 3-55 添加 NCP 打印机

用于以下选项的文本字段会出现：

- 服务器 — 打印机所连接的 NCP 系统的主机名或 IP 地址。
- 队列 — NCP 系统上的打印机的远程队列。
- 用户 — 你要使用打印机所必须登录的用户名。
- 口令 — 为以上“用户”字段指定的口令。

3.20.6 添加 JetDirect 打印机

要添加 JetDirect 打印机，点击打印机配置工具主窗口上的“新建”按钮。如图 3-48 所示的窗口就会出现。点击“前进”来继续。

在如图 3-50 所示窗口中的“名称”文本字段中输入一个独特名称。打印机名称不能包含空格，必须以字母开头。打印机名称可以包含字母、数字、短线（-）和下划线（_）。你还可以输入打印机的简短描述，其中可以包含空格。

从“选择队列类型”菜单中选择“联网的 JetDirect”，然后点击“前进”。

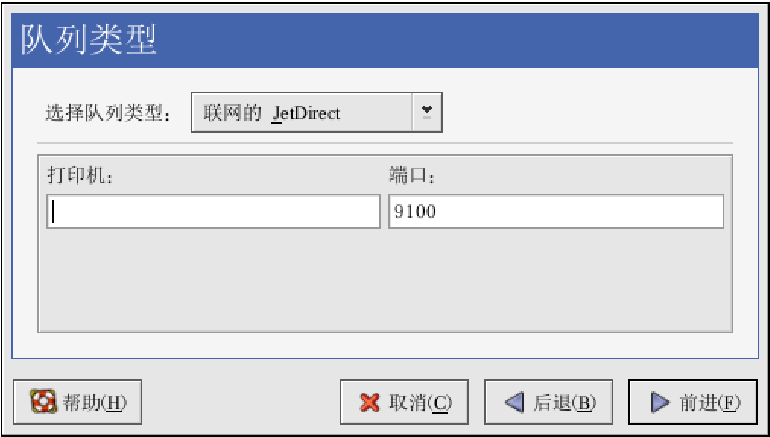


图 3-56 添加 JetDirect 打印机

用于以下选项的文本字段会出现：

- 打印机 — JetDirect 打印机的主机名或 IP 地址。
- 端口 — JetDirect 打印机监听打印作业的端口。默认端口为 9100。

3.20.7 选择打印机型号和结束

选择了打印机的队列类型后，下一步就是选择打印机型号。

你会看到一个和图 3-57 相似的窗口。如果它没有被自动检测到，从列表中选择它。打印机按照生产厂家分类。从拉下菜单中选择打印机的生产厂家的名称。每当选择了一个不同的生产厂家后，打印机型号列表都会被更新。从列表中选择打印机型号。

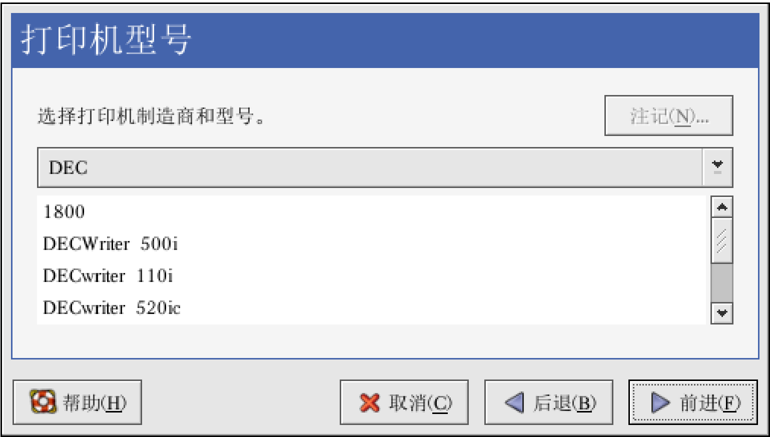


图 3-57 选择打印机型号

推荐的打印驱动程序是根据选定的打印机型号而选择的。打印驱动程序把你想打印的数据处理成打印机能够理解的格式。由于本地打印机是直接连接到你的计算机上的，你需要一个打印驱动程序来处理发送给打印机的数据。

如果你在配置远程打印机（IPP、LPD、SMB 或 NCP），远程打印服务器通常有它自己的打印驱动程序。如果在你的本地计算机上选择额外的打印驱动程序，数据就会被多次过滤并被转换成打印机所无法理解的格式。

要确定数据不会被多次过滤，首先请在生产厂家上选择“通用”，在打印机型号上选择“原始打印队列”或“Postscript 打印机”。应用了改变后，打印一张测试页来试验新配置。如果测试失败，远程打印服务器可能没有配置打印驱动程序。试着根据远程打印机的生产厂家和型号来选择打印驱动程序，应用改变后，再打印一张测试页。

3.20.7.1 确认打印机配置

最后一步是确认你的打印机配置。如果设置正确，则点击“应用”来添加打印队列，否则，点击“后退”来修改打印机配置。

在主窗口中点击“应用”按钮来保存你的改变并重新启动打印机守护进程。

应用了改变后，打印一张测试页来确定配置的正确性。

如果你需要打印基本的 ASCII 集合以外的字符（包括用于日文之类的语言中的字符），你必须回顾一下你的驱动程序选项，并选择“预绘制 Postscript”。如果你在添加了打印队列后编辑它，你还可以配置纸张大小之类的选项。

3.20.8 打印测试页

配置了打印机后，你应该打印一张测试页来确定打印机能够正常运行。要打印测试页，从打印机列表中选择你想试验的打印机，然后从“测试”拉下菜单中选择合适的测试页。

如果你改变了打印驱动程序或修改了驱动程序选项，你应该打印一张测试页来测试不同的配置。

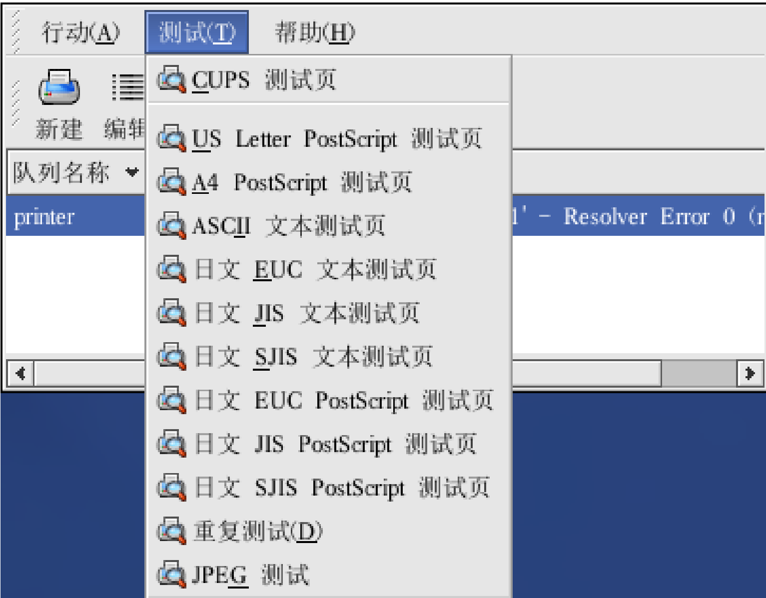


图 3-58 测试页选项

3.20.9 修改现存打印机

要删除某个现存打印机，选择这个打印机，然后点击工具栏上的“删除”按钮。打印机就会从打印机列表中删除。点击“应用”按钮来保存改变并重新启动打印机守护进程。

要设置默认的打印机，从打印机列表中选择打印机，然后点击工具栏上的“默认”按钮。默认的打印机图标会出现在列表中默认打印机的“默认”列中。IPP 浏览中得出的队列打印机不能在打印机配置工具中被设置为默认打印机。要使 IPP 打印机成为默认选择，请添加它然后在把它选为默认，或使用 GNOME 打印管理器来把它设置为默认。要启动 GNOME 打印管理器，选择“主菜单 －> 系统工具 －> 打印管理器”。右击队列名称，然后选择“设为默认”。在 GNOME 打印管理器中设置默认打印机只会为配置它的用户改变默认设置；它不是系统全局的设置。

添加了打印机后，你还可以编辑它们的设置。从打印机列表中选择要编辑的打印机，然后点击“编辑”按钮。如图 3-59 所示的带活页标签的窗口就会出现。该窗口包含选中打印机的当前值。进行了必要改变后，点击“确定”按钮。点击打印机配置工具主窗口中的“应用”来保存改变并重新启动打印机守护进程。

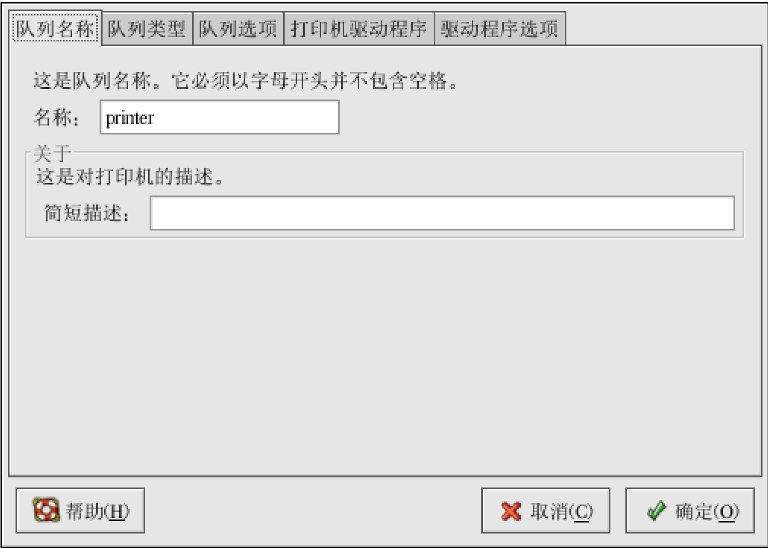


图 3-59 编辑打印机

3.20.9.1 队列名称

要重命名打印机或改变它的简短描述，改变“队列名称”标签中的值。点击“确定”来返回到主窗口。打印机的名称应该会在打印机列表中被改变。点击“应用”来保存改变并重新启动打印机守护进程。

3.20.9.2 队列类型

“队列类型”标签显示了在添加打印机和它的设置时选中的队列类型。你可以改变打印机类型或仅改变它的设置。修改后，点击“确定”来返回到主窗口。点击“确定”来保存改变并重新启动打印守护进程。

根据你选择的队列类型，不同的选项会被显示。

3.20.9.3 打印机驱动程序

“打印机驱动程序”标签显示了当前使用的打印驱动程序。如果它被改变

了，点击“确定”来回到主窗口。点击“应用”来保存改变并重新启动打印守护进程。

3.20.9.4 驱动程序选项

“驱动程序选项”标签显示了高级打印机选项。每个打印驱动器的选项会略有不同。公用选项有：

- 如果基本 ASCII 集合之外的字符被发送给打印机却没有被正确打印（如日文字符），你应该选择“预绘制 Postscript”。该选项预先绘制非标准的 PostScript 字体，因此它们能够被正确打印。

如果打印机不支持你试图打印的字体，你可以试着选择这个选项。例如，选择这个选项来把日文字体打印到非日文打印机上。

执行以上行动需要多花些时间。除非你在打印正确字体时遇到问题，请不要使用这个选项。

还有，如果打印机无法处理 PostScript 级别 3 时，你也可以选择这个选项。该选项会把它转换成 PostScript 级别 1。

- GhostScript 预过滤 — 允许你在打印机无法处理某些 PostScript 级别时选择“无预过滤”、“转换到 PS 级别 1”、或“转换到 PS 级别 2”。该选项只在 CUPS 打印系统中使用了 PostScript 驱动程序时才可用。

- 纸张大小允许你选择纸张的大小。该选项包括 US Letter、US Legal、A3 和 A4。

- 有效的过滤区默认为 C。如果要打印日文字符，选择“ja_JP”。否则，接收默认的 C 语区。

- 介质源默认为“打印机默认”。这个选项可以被改为使用另一个托盘中的纸张。

要修改驱动程序选项，点击“确定”来返回到主窗口。点击“应用”来保存改变并重新启动打印守护进程。

3.20.10 保存配置文件

当你使用打印机配置工具保存打印机配置时，应用程序就会创建它自己的配置文件。这个配置文件被用来创建 /etc/cups 目录中的文件。你可以使用命令行选项来保存或恢复打印机配置工具文件。如果 /etc/cups 目录被保存然后被恢复到同一位置，打印机配置也不会被恢复，这是由于打印机守护进程在每次重新启动时都会从打印机配置工具的特殊配置文件中创建一个新的 /etc/printcap 文件。当创建系统配置文件的备份时，使用以下方法来保存打印机配置文件。

要保存你的打印机配置，以根用户身份键入：

```
/usr/sbin/system-config-printer-tui --Xexport > settings.xml
```

你的配置就会被保存到 settings.xml 文件中。

如果这个文件被保存，它可以被用来恢复打印机设置。这在打印机配置被删除的情况下；或在重新安装了 GTES10 的情况下；或在多个系统上需要同一打印机配置的情况下特别有用。在重新安装前，这个文件应该被保存在不同的系统上。要恢复配置，以根用户身份键入以下命 令：

```
/usr/sbin/system-config-printer-tui --Ximport < settings.xml
```

如果你已有了一个配置文件（你已经在系统上配置了一个或多个打印机），并想试图导入另一个配置文件，现存的配置文件就会被覆盖。如果你想保留现存配置，并在保存的文件中添加配置，你可以使用以下命令来合并文件（以根用户身份）：

```
/usr/sbin/system-config-printer-tui --Ximport --merge < settings.xml
```

然后，你的打印机列表就会包含你在系统上配置的打印机以及你从保存的配置文件中导入的打印机。如果导入的配置文件中有一个和系统上现存打印队列同名的队列，导入文件中的队列就会超越现存打印机。

导入了配置文件（不管有没有 merge 命令）后，你都必须重新启动守护进程。请执行以下命令：

```
/sbin/service cups restart
```

3.20.11 命令行配置

如果你没有安装 X，并且不想使用基于文本的程序，你可以通过命令行来添加打印机。这种方法在你从脚本中或 kickstart 安装的 %post 部分里添加打印机的时候很有用。

3.20.11.1 添加本地打印机

要添加打印机，运行：

```
system-config-printer-tui --Xadd-local options
```

其选项有：

- --device=node

（必需）要使用的设备节点。例如：/dev/lp0。

- --make=make

（必需）IEEE 1284 MANUFACTURER 字符串或 foomatic 数据库中的打印机生产厂商的名称（若无 manufacturer 字符串）。

- --model=model

（必需） IEEE 1284 MODEL 字符串或 foomatic 数据库中列出的打印机型号（若无 model 字符串）。

- --name=name

（可选）新队列的名称。如果没有给定，将会使用基于设备节点（如 "lp0"）的名称。

- --as-default

（可选）把它设为默认队列。

添加了打印机后，使用以下命令来启动或重新启动打印机守护进程：

```
service cups restart
```

3.20.11.2 删除本地打印机

你还可以通过命令行来删除打印机队列。

要以根用户身份来删除某个打印机队列，运行：

```
system-config-printer-tui --Xremove-local options
```

其选项有：

- --device=node

（必需）所用的设备节点，如 /dev/lp0。

- --make=make

（必需）IEEE 1284 MANUFACTURER 字符串或 foomatic 数据库中的打印机生产厂商的名称（若无 manufacturer 字符串）。

- --model=model

（必需） IEEE 1284 MODEL 字符串或 foomatic 数据库中列出的打印机型号（若无 model 字符串）。

从打印机配置工具配置中删除了打印机后，使用以下命令来重新启动打印机守护进程而使改变生效：

```
service cups restart
```

如果所有打印机都被删除，并且你不打算再运行打印机守护进程，请执行以下命令：

```
service cups stop
```

3.20.11.3 设置默认打印机

要设置默认打印机，使用以下命令，并指定 queuename：

```
system-config-printer-tui --Xdefault --queue=queuename
```

3.20.12 管理打印作业

当你给打印机守护进程发送打印作业时（例如从 Emacs 中打印文本文件或从 The GIMP 中打印图像），这个打印作业被添加到打印假脱机队列中。打印假脱机队列是一个被发送给打印机的打印作业以及每个打印请求的信息的列表。这些信息包括打印请求的状态、发送请求的用户名、发送请求的系统主机名、作业号码等等。

如果你运行的是图形化桌面环境，点击面板上的“打印机管理器”图标来启动 GNOME 打印管理器，如图 3-60 所示。

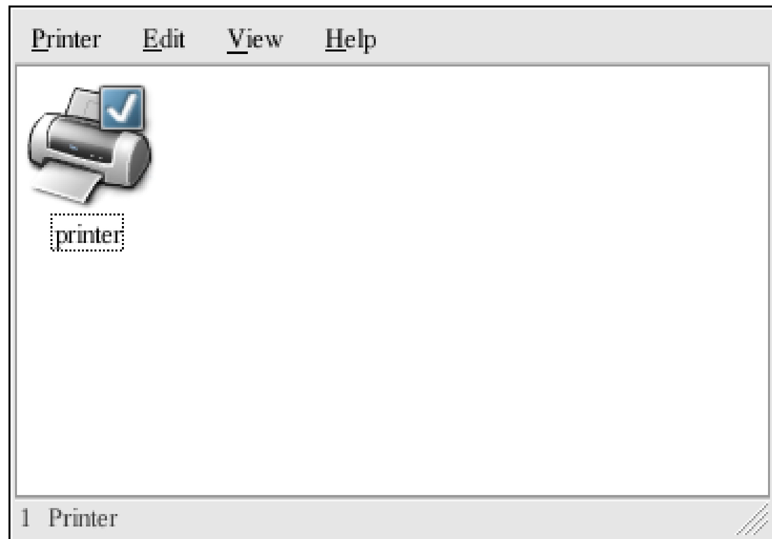


图 3-60 GNOME 打印管理器

它还可以从面板上启动。点击“主菜单 —> 系统工具 —> 打印管理器”。

要改变打印机设置，右击打印机图标，然后选择“属性”。打印机配置工具就会被启动。

双击一个已配置的打印机来查看打印假脱机，如图 3-61 所示。

Printer Edit View Help

Document	Owner	Job Number	Size	Time Submitted
testprint.ps	root	1	Unknown	2003

1 job in queue "printer"

图 3-61 打印作业列表

要取消在 GNOME 打印管理器中列出的某一作业，从列表中选择它，然后选择“编辑 —> 取消文档”。

如果打印假脱机中有活跃的打印作业，打印机通知图标可能会出现在桌面面板上的“面板通知区域”，如图 3-62 所示。因为它每隔五秒探测一次打印作业，较短的打印作业可能不会显示图标。



图 3-62 打印机通知图标

点击打印机通知图标会启动 GNOME 打印管理器来显示当前打印作业的列表。

面板上还有一个“打印管理器”图标。要从 Nautilus 打印某文件，浏览该文件的位置，把它拖放到面板上的“打印管理器”图标。如图 3-63 所示的窗口就会出现。点击“确定”来开始打印这个文件。

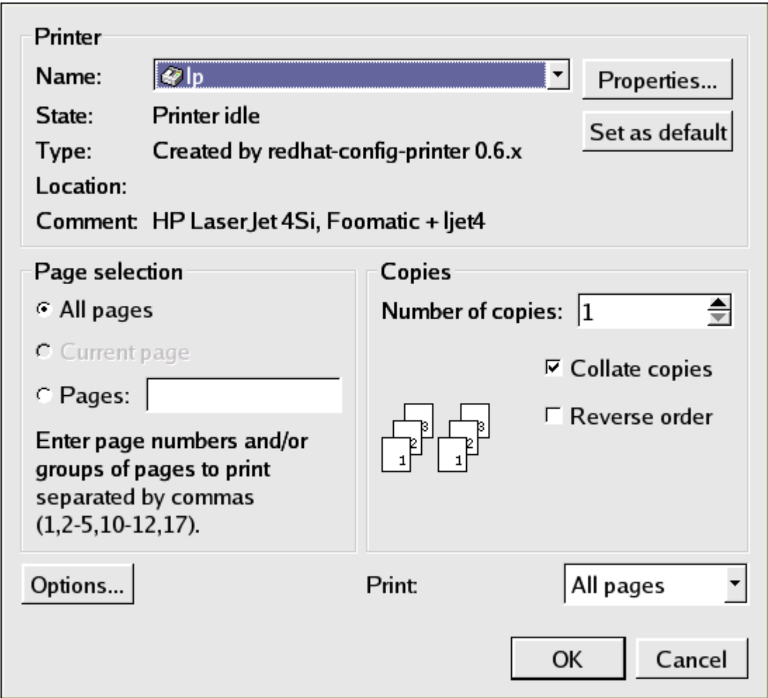


图 3-63 打印校验窗口

要从 shell 提示查看打印假脱机中的打印作业列表，键入 lpq 命令。最后几行和以下输出相似：

```
Rank   Owner/ID               Class  Job Files        Size Time
active user@localhost+902      A     902 sample.txt   2050 01:20:46
```

如果你想取消某个打印作业，使用 lpq 命令找出这个作业的号码，然后使用 lprm 作业号码。例如，lprm 902 会取消 例 36-1 所示的打印作业。你必须具备正确的权限才能够取消某个打印作业。除非你在打印机所连接的计算机上登录为根用户，你不能取消被其他用户开始的打印作业。

你还可以直接从 shell 提示下打印文件。例如，lpr sample.txt 命令会打印 sample.txt 这个文本文件。打印过滤器决定文件的类型并将其转换成打印机能够理解的格式。

3.20.13 共享打印机

打印机配置工具的共享配置选项能力只有在使用 CUPS 打印系统时才有效。

允许网络上不同计算机上的用户打印到你的系统上配置的打印机叫做“共享（sharing）打印机”。按默认设置，使用打印机配置工具配置的打印机不是共享打印机。

要共享一个配置了的打印机，启动打印机配置工具，从列表中选择一个打印机。然后选择“行动 —> 共享”。

在“队列”活页标签上，选择使队列可被其他用户利用的选项。



图 3-64 队列选项

选择了要共享队列后，按照默认设置，所有主机都会被允许打印到共享打印机。允许网络上的所有系统都能够打印到队列中可能会很危险，特别是在系统直接连接到互联网的情况下。推荐你改变这个选项，方法是：选择“所有主机”，点击“编辑”按钮来显示如图 3-65 所示的窗口。

如果你在打印服务器上配置了防火墙，它必须能够在进入的 UDP 端口

631 上发送和接收连接。如果你在客户（发送打印请求的计算机）上配置了防火墙。它必须被允许在端口 631 上发送和接收连接。



图 3-65 允许的主机

“常规”标签为所有打印机配置设置，包括那些打印机配置工具中看不到的打印机。其中有两个选项：

- 自动寻找远程共享队列 — 被默认选择。这个选项启用 IPP 浏览，这意味着当网络上其它机器广播它们拥有的队列时，这些队列会被自动添加到系统的打印机列表中；由 IPP 浏览所发现的打印机不需要额外的配置。该选项不自动共享本地系统上配置的打印机。

- 启用 LPD 协议 — 该选项允许打印机使用 cups-lpd 服务从配置使用 LPD 协议的客户中接收打印作业。cups-lpd 服务是一种 xinetd 服务。



图 3-66 系统范围的共享选项

3.21 自动化的任务

在 Linux 中，任务可以被配置在指定的时间段、指定的日期、或系统平均载量低于指定的数量时自动运行。GTES10 预配置了对重要系统任务的运行，以便使系统能够时时被更新。譬如，被 locate 命令使用的 slocate 数据库每日都被更新。系统管理员可使用自动化的任务来执行定期备份、监控系统、运行定制脚本等等。

GTES10 随带几个自动化任务的工具：cron、at、和 batch。

3.21.1 cron

cron 是一个可以用来根据时间、日期、月份、星期的组合来调度对重复任务的执行的守护进程。

cron 假定系统持续运行。如果当某任务被调度时系统不在运行，该任务就

不会被执行。

要使用 cron 服务，你必须安装了 vixie-cron RPM 软件包，而且必须在运行 crond 服务。要判定该软件包是否已安装，使用 rpm -q vixie-cron 命令。要判定该服务是否在运行，使用 /sbin/service crond status 命令。

3.21.1.1 配置 cron 任务

cron 的主配置文件是 /etc/crontab，它包括下面几行：

```
SHELL=/bin/bash

PATH=/sbin:/bin:/usr/sbin:/usr/bin

MAILTO=root

HOME=/

# run-parts

01 * * * * root run-parts /etc/cron.hourly

02 4 * * * root run-parts /etc/cron.daily

22 4 * * 0 root run-parts /etc/cron.weekly

42 4 1 * * root run-parts /etc/cron.monthly
```

前四行是用来配置 cron 任务运行环境的变量。SHELL 变量的值告诉系统要使用哪个 shell 环境（在这个例子里是 bash shell）；PATH 变量定义用来执行命令的路径。cron 任务的输出被邮寄给 MAILTO 变量定义的用户名。如果 MAILTO 变量被定义为空白字符串（MAILTO=""），电子邮件就不会被寄出。HOME 变量可以用来设置在执行命令或脚本时使用的主目录。

/etc/crontab 文件中的每一行都代表一项任务，它的格式是：

```
minute   hour   day   month   dayofweek   command
```

- minute — 分钟，从 0 到 59 之间的任何整数
- hour — 小时，从 0 到 23 之间的任何整数

- day — 日期，从 1 到 31 之间的任何整数（如果指定了月份，必须是该月份的有效日期）
- month — 月份，从 1 到 12 之间的任何整数（或使用月份的英文简写如 jan、feb 等等）
- dayofweek — 星期，从 0 到 7 之间的任何整数，这里的 0 或 7 代表星期日（或使用星期的英文简写如 sun、mon 等等）
- command — 要执行的命令（命令可以是 ls /proc >> /tmp/proc 之类的命令，也可以是执行你自行编写的脚本的命令。）

在以上任何值中，星号（*）可以用来代表所有有效的值。譬如，月份值中的星号意味着在满足其它制约条件后每月都执行该命令。

整数间的短线（-）指定一个整数范围。譬如，1-4 意味着整数 1、2、3、4。

- 用逗号（,）隔开的一系列值指定一个列表。譬如，3, 4, 6, 8 标明这四个指定的整数。
- 正斜线（/）可以用来指定间隔频率。在范围后加上 /<integer> 意味着在范围内可以跳过 integer。譬如，0-59/2 可以用来在分钟字段定义每两分钟。间隔频率值还可以和星号一起使用。例如，*/3 的值可以用在月份字段中表示每三个月运行一次任务。
- 开头为井号（#）的行是注释，不会被处理。

如你在 /etc/crontab 文件中所见，它使用 run-parts 脚本来执行 /etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly 和 /etc/cron.monthly 目录中的脚本，这些脚本被相应地每小时、每日、每周、或每月执行。这些目录中的文件应该是 shell 脚本。

如果某 cron 任务需要根据调度来执行，而不是每小时、每日、每周、或每月地执行，它可以被添加到 /etc/cron.d 目录中。该目录中的所有文件使用和 /etc/crontab 中一样的语法。范例请参见 例 37-1。

```
# record the memory usage of the system every monday

# at 3:30AM in the file /tmp/meminfo
```

```
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo

# run custom script the first day of every month at 4:10AM

10 4 1 * * /root/scripts/backup.sh
```

根用户以外的用户可以使用 crontab 工具来配置 cron 任务。所有用户定义的 crontab 都被保存在 /var/spool/cron 目录中，并使用创建它们的用户身份来执行。要以某用户身份创建一个 crontab 项目，登录为该用户，然后键入 crontab -e 命令，使用由 VISUAL 或 EDITOR 环境变量指定的编辑器来编辑该用户的 crontab。该文件使用的格式和 /etc/crontab 相同。当对 crontab 所做的改变被保存后，该 crontab 文件就会根据该用户名被保存，并写入文件 /var/spool/cron/username 中。

cron 守护进程每分钟都检查 /etc/crontab 文件、etc/cron.d/ 目录、以及 /var/spool/cron 目录中的改变。如果发现了改变，它们就会被载入内存。这样，当某个 crontab 文件改变后就不必重新启动守护进程了。

3.21.1.2 控制对 cron 的使用

/etc/cron.allow 和 /etc/cron.deny 文件被用来限制对 cron 的使用。这两个使用控制文件的格式都是每行一个用户。两个文件都不允许空格。如果使用控制文件被修改了，cron 守护进程（crond）不必被重启。使用控制文件在每次用户添加或删除一项 cron 任务时都会被读取。

无论使用控制文件中的规定如何，根用户都总是可以使用 cron。

如果 cron.allow 文件存在，只有其中列出的用户才被允许使用 cron，并且 cron.deny 文件会被忽略。

如果 cron.allow 文件不存在，所有在 cron.deny 中列出的用户都被禁止使用 cron。

3.21.1.3 启动和停止服务

要启动 cron 服务，使用 /sbin/service crond start 命令。要停止该服务，使用 /sbin/service crond stop 命令。推荐你在引导时启动该服务。

3.21.2 at 和 batch

cron 被用来调度重复的任务，at 命令被用来在指定时间内调度一次性的任务。batch 命令被用来在系统平均载量降到 0.8 以下时执行一次性的任务。

要使用 at 或 batch 命令，你必须安装了 at RPM 软件包，并且 atd 服务必须在运行。要判定该软件包是否被安装了，使用 rpm -q at 命令。要判定该服务是否在运行，使用 /sbin/service atd status 命令。

3.21.2.1 配置 at 作业

要在某一指定时间内调度一项一次性作业，键入 at time 命令。这里的 time 是执行命令的时间。

time 参数可以是下面格式中任何一种：

- HH:MM 格式 — 譬如，04:00 代表 4:00AM。如果时间已过，它就会在第二天的这一时间执行。
- midnight — 代表 12:00AM。
- noon — 代表 12:00PM。
- teatime — 代表 4:00PM。
- 英文月名 日期 年份 格式— 譬如，January 15 2002 代表 2002 年 1 月 15 日。年份可有可无。
- MMDDYY、MM/DD/YY、或 MM.DD.YY 格式 — 譬如，011502 代表 2002 年 1 月 15 日。
- now + 时间 — 时间以 minutes、hours、days、或 weeks 为单位。譬如，now + 5 days 代表命令应该在 5 天之后的此时此刻执行。

时间必须要被先指定，接着是可有可无的日期。

键入了 at 命令和它的时间参数后，at> 提示就会出现。键入要执行的命令，按 [Enter] 键，然后键入 Ctrl-D。你可以指定多条命令， 方法是键入

每一条命令后按 [Enter] 键。键入所有命令后，按 [Enter] 键转入一个空行，然后再键入 Ctrl-D。或者，你也可以在提示后输入 shell 脚本，在脚本的每一行后按 [Enter] 键，然后在空行处键入 Ctrl-D 来退出。如果输入的是脚本，所用的 shell 就会是用户的 SHELL 环境变量中设置的值，用户的登录 shell，或是 /bin/sh（使用最先发现的）。

如果这组命令或脚本试图在标准输出中显示信息，该输出会用电子邮件方式被邮寄给用户。

使用命令 atq 来查看等待运行的作业。

at 命令的用法能够被制约。

3.21.2.2 配置 batch 作业

要在系统平均载量降到 0.8 以下时执行某项一次性的任务，使用 batch 命令。

键入 batch 命令后，at> 提示就会出现。键入要执行的命令，按 [Enter] 键，然后键入 Ctrl-D。你可以指定多条命令，方法是键入每一条命令后按 [Enter] 键。键入所有命令后，按 [Enter] 键转入一个空行，然后再键入 Ctrl-D。或者， 你也可以在提示后输入 shell 脚本，在脚本的每一行后按 [Enter] 键，然后 在空行处键入 Ctrl-D 来退出。如果输入的是脚本，所用的 shell 就会是用户的 SHELL 环境变量中设置的值，用户的登录 shell，或是 /bin/sh（使用最先发现的）。系统平均载量一降到 0.8 以下，这组命令或脚本就会被执行。

如果这组命令或脚本试图在标准输出中显示信息，该输出会用电子邮件方式被邮寄给用户。

使用命令 atq 来查看等待运行的作业。

3.21.2.3 查看等待运行的作业

要查看等待运行的 at 和 batch 作业，使用 atq 命令。它显示一列等待运行的作业，每项作业只占据一行。每一行的格式都是：作业号码、日期、

小时、作业类别、以及用户名。用户只能查看他们自己的作业。如果根用户执行 atq 命令，所有用户的全部作业都会被显示。

3.21.2.4 其它的命令行选项

at 和 batch 的其它命令行选项包括：

选项	描述
-f	从文件中读取命令或 shell 脚本，而非在提示后指定它们。
-m	在作业完成后，给用户发送电子邮件。
-v	显示作业将被执行的时间。

表 3-5 at 和 batch 的命令行选项

3.21.2.5 控制对 at 和 batch 的使用

/etc/at.allow 和 /etc/at.deny 文件可以用来限制对 at 和 batch 命令的使用。这两个使用控制文件的格式都是每行一个用户。两个文件都不允许使用空白字符。如果使用控制文件被修改了，at 守护进程（atd） 不必被重启。每次用户试图执行 at 或 batch 命令时，使用控制文件都会被读取。

不论使用控制文件如何规定，根用户都总是可以执行 at 和 batch 命令。

如果 at.allow 文件存在，只有其中列出的用户才能使用 at 或 batch 命令，at.deny 文件会被忽略。

如果 at.allow 文件不存在，所有在 at.deny 文件中列出的用户都被禁止使用 at 和 batch 命令。

3.21.2.6 启动和停止服务

要启动 at 服务，使用 /sbin/service atd start 命令。要停止该服务， 使用 /sbin/service atd stop 命令。建议你在引导时启动该服务。

3.22 日志文件

日志文件（Log files）是包含系统消息的文件，包括内核、服务、在系统上运行的应用程序等。不同的日志文件记载不同的信息。例如，有的是默认的系统日志文件，有的仅用于安全消息，有的记载 cron 任务的日志。

当你在试图诊断和解决系统问题时，如试图载入内核驱动程序或寻找对系统未经授权的使用企图时，日志文件会很有用。本节讨论要到哪里去寻找日志文件，如何查看日志文件，以及在日志文件中查看什么。

某些日志文件被叫做 syslogd 的守护进程控制。被 syslogd 维护的日志消息列表可以在 /etc/syslog.conf 配置文件中找到。

3.22.1 定位日志文件

多数日志文件位于 /var/log/ 目录中。某些程序如 httpd 和 samba 在 /var/log/ 中有单独的存放它们自己的日志文件的目录。

注意，日志文件目录中会有多个后面带有数字的文件。这些文件是在日志文件被循环时创建的。日志文件被循环使用，因此文件不会变得太大。logrotate 软件包中包含一个能够自动根据 /etc/logrotate.conf 配置文件和 /etc/logrotate.d 目录中的配置文件来循环使用日志文件的 cron 任务。按照默认配置，日志每周都被循环，并被保留四周之久。

3.22.2 查看日志文件

多数日志文件使用纯文本格式。你可以使用任何文本编辑器如 Vi 或 Emacs 来查看它们。某些日志文件可以被系统上所有用户查看；不过，你需要拥有根特权来阅读多数日志文件。

要在互动的、真实时间的应用程序中查看系统日志文件，使用 日志查看器。要启动这个应用程序，点击面板上的“主菜单 —> 系统工具 —> 系统日志”，或在 shell 提示下键入 system-logviewer 命令。

这个应用程序只能显示存在的日志文件；因此，其列表可能会与图 3-67 所示的略有不同。

要过滤日志文件的内容来查找关键字，在“过滤：”文本字段中输入关键字，然后点击“过滤器”。点击“重设”来重设内容。

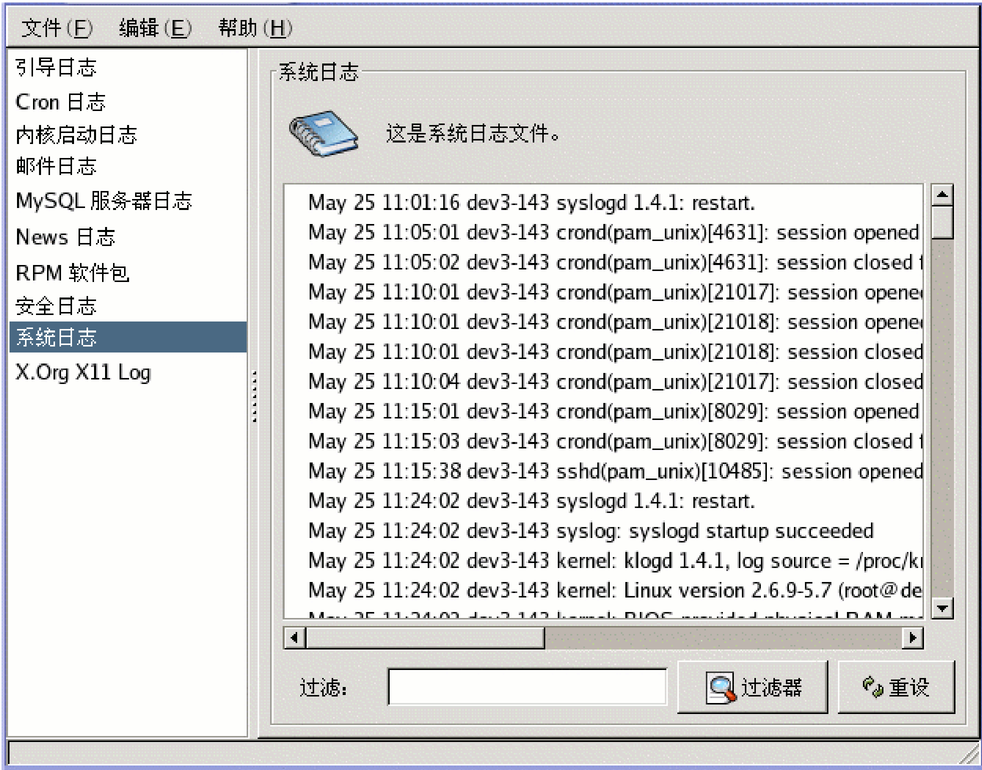


图 3-67 日志查看器

按照默认设置，当前的可查看的日志文件每隔 30 秒被刷新一次。要改变刷新率，从下拉菜单中选择“编辑 —> 首选项”。如图 3-68 所示的窗口会出现。在“日志文件”标签中，点击 刷新率旁边的上下箭头来改变它。点击 “关闭”来返回到主窗口。刷新率会被立即改变。要手工刷新当前可以查看的文件，选择“文件 —> 即刻刷新”或按 [Ctrl]-[R]。

你可以在首选项的“日志文件”活页标签中改变日志文件的位置。从列表

中选择日志文件，然后点击“编辑”按钮。键入日志文件的新位置，或点击“浏览”按钮来从文件选择对话框中定位文件位置。点击“确定”来返回到首选项窗口，然后点击“关闭”来返回到主窗口。

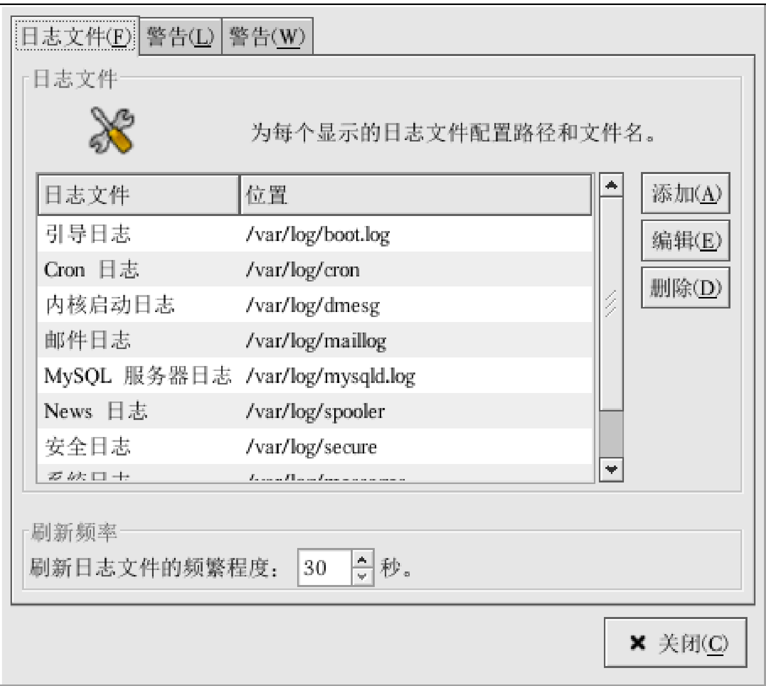


图 3-68 日志文件的位置

3.22.3 添加日志文件

要在列表中添加一个日志文件，选择“编辑 —> 首选项”，然后点击“日志文件”活页标签中的“添加”按钮。

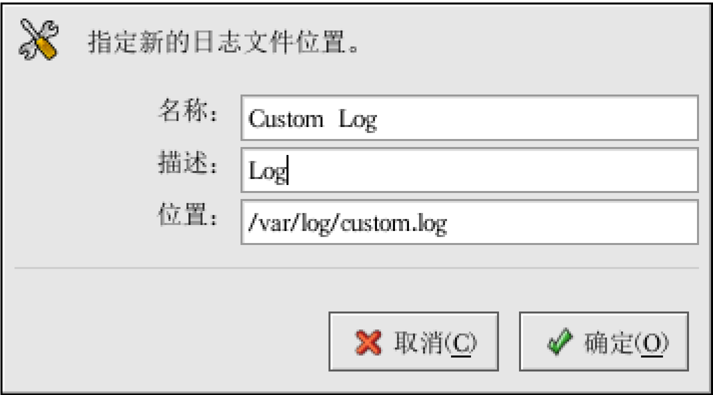


图 3-69 添加日志文件

提供要添加的日志文件的名称、描述和位置。点击了“确定”后，该文件若存在就会立即被添加到查看区域。

3.22.4 检查日志文件

日志查看器能够被配置来在包含报警词的行旁边显示一个报警图标；在包含警告词的行旁边显示一个警告图标。

要添加报警词，从拉下菜单中选择“编辑 —> 首选项”，然后点击“报警”活页标签。点击“添加”按钮来添加报警词。要删除一个报警词，从列表中选择它，然后点击“删除”。

报警图标 显示在包含报警词的行的左侧。

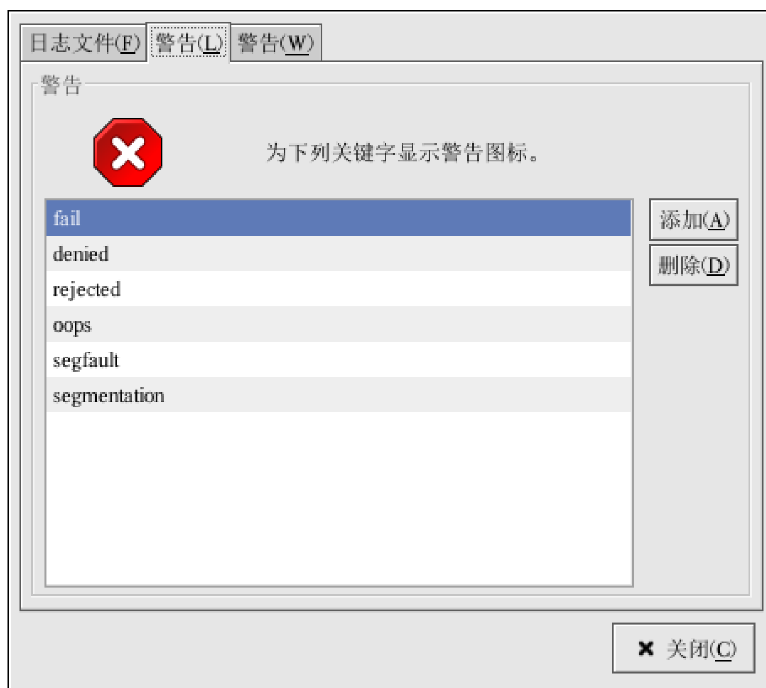


图 3-70 警告

要添加警告词，从拉下菜单中选择“编辑 —> 首选项”，然后点击“警告”标签。点击“添加”按钮来添加警告词。要删除一个警告词，从列表中选择它，然后点击“删除”。

警告图标 ⚠显示在包含警告词的行的左侧。

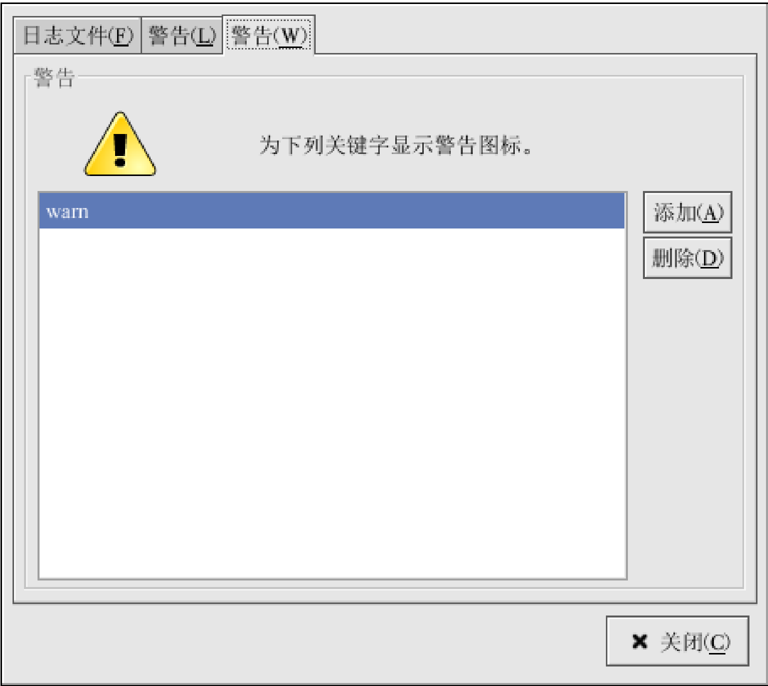


图 3-71 警告

3.23 升级内核

为了确保内核的完整性和对它所支持的硬件的兼容性，GTES10 内核由 Turbolinux 内核小组定制建构。在内核被 Turbolinux 发行之前，它一定要通过一系列严格的质量保证测试。

GTES10 内核使用 RPM 格式打包，因而它们易于升级和校验。例如，由 Turbolinux, Inc. 发行的 kernel RPM 软件包被安装后，initrd 映像会被创建；这样，在你安装了不同的内核后，你就没必要使用 mkinitrd 命令。它还会修改引导装载程序的配置文件来包括这个新内核。

3.23.1 内核软件包总览

GTES10 包含以下内核软件包（某些可能不适用于你的体系）：

- kernel — 包含内核和以下关键功能：

对 x86 和 Athlon 系统的单处理器支持（可以在多处理器系统上运行，但是只利用一个处理器）

对所有其它体系的多处理器支持

对于 x86 系统，只能利用最先的 4GB 内存；对于拥有大于 4GB 内存的 x86 系统，请使用 kernel-hugemem 软件包。

- kernel-hugemem — （只用于 i686 系统）kernel 软件包启用的选项之外附加的选项。关键配置选项如下所示：

对大于 4GB 内存的支持（在 x86 中可高达 16GB）

PAE（物理地址扩展），或 x86 处理器上支持 PAE 的三级调页

多处理器支持

4GB/4GB 分割 — 在 x86 系统上，4GB 虚拟地址空间用于内核，将近 4GB 的空间用于每个用户进程

- kernel-BOOT — 仅在安装中被使用。
- kernel-pcmcia-cs — 包含对 PCMCIA 卡的支持。
- kernel-smp — 包含用于多处理器系统的内核。以下是它的关键特性：

多处理器支持

对大于 4GB 内存的支持（x86 系统中高达 64GB）

PAE（物理地址扩展），或 x86 处理器上支持 PAE 的三级调页

- kernel-source — 包含 Linux 内核的源码文件
- kernel-util — 包含能够用来控制内核或系统硬件的工具程序。
- kernel-unsupported — 某些体系有

因为 GTES10 不可能包含对没件可用硬件的支持，该软件包所包含的模块

在安装中或安装后将不会被 Turbolinux, Inc. 支持。它在安装过程中不会被安装；它必须在安装后被安装。不被支持的软件包中的驱动程序是按照尽力而为的原则提供的 — 更新和修正可能会也可能不会被提供。

3.23.2 准备升级

在你升级内核之前，你应该先采取几项预防措施。如果系统有一个软盘驱动器，那么第一步就是确定你有一张适用于你的系统的可运行的引导盘以防万一出现问题。如果引导装载程序没有被正确配置来引导新内核，除非你有引导盘，否则就无法引导系统。

要创建引导盘，登录为根用户，然后在 shell 提示下键入以下命令：

```
/sbin/mkbootdisk `uname -r`
```

在继续前，使用引导盘来重新引导你的机器以校验该软盘的可运行性。

但愿你不必使用引导盘，但是你应该把它存放在一个安全的地方以防万一。

要判定你已安装了哪些内核软件包，在 shell 提示下执行下面的命令：

```
rpm -qa | grep kernel
```

依据你的系统体系而定（你的版本号码和软件包可能不同），该命令的输出会包括部分或全部在以下列出的软件包：

```
kernel-2.4.21-1.1931.2.399.ent

kernel-source-2.4.21-1.1931.2.399.ent

kernel-utils-2.4.21-1.1931.2.399.ent

kernel-pcmcia-cs-3.1.31-13

kernel-smp-2.4.21-1.1931.2.399.ent
```

从输出中，你可以判定你需要下载哪些软件包来执行内核升级。对于单处理器系统而言，只有 kernel 软件包是必需的。

每个内核软件包的文件名中都包含它所建构的体系名称。文件名的格式

为：kernel-<variant>-<version>.<arch>.rpm，这里的 <variant> 是指 smp、utils 等等。<arch> 是以下一种：

- x86_64 用于 AMD64 体系。
- ia64 用于 Intel® Itanium™ 体系。
- ppc64pseries 用于 IBM® eServer™ pSeries™ 体系。
- ppc64iseries 用于 IBM® eServer™ iSeries™ 体系。
- s390 用于 IBM® S/390® 体系。
- s390x 用于 IBM® eServer™ zSeries® 体系。

x86 类别：x86 内核为不同的 x86 版本进行了优化处理。其选项如下：

- athlon 用于 AMD Athlon® 和 AMD Duron® 系统
- i686 用于 Intel® Pentium® II, Intel® Pentium® III 和 Intel® Pentium® 4 系统

3.23.3 下载升级了的内核

要判定是否有可用于你的系统的升级内核，方法有好几种。

安全勘误：访问以下位置来找出安全勘误的信息，包括修正安全问题的内核升级：

http://www.turbolinux.com.cn/

使用 Turbolinux 网络来下载内核 RPM 软件包并安装它们。Turbolinux 网络能够下载最新的内核；升级系统上的内核；如果必要，创建初始 RAM 磁盘映像；并配置引导装载程序来引导新内核。要获取更多信息，请访问网站： http://www.turbolinux.com.cn/

3.23.4 执行升级

检索到所有必要的软件包后，你就可以开始升级现存内核了。在 shell 提示下登录为根用户，转换到包含内核 RPM 软件包的目录中，遵循以下步

骤：

- 使用 rpm 命令的 -i 选项来保留旧内核。如果你使用了 -U 选项来升级 kernel 软件包，它会覆盖当前安装了的内核。该命令为（内核版本会有所不同）：

```
rpm -ivh kernel-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

- 如果系统是多处理器系统，还需安装 kernel-smp 软件包（内核版本会有所不同）：

```
rpm -ivh kernel-smp-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

- 如果系统是基于 i686 的，并包含超过 4GB 的内存，还需安装为 i686 体系建构的 kernel-bigmem 软件包（内核版本会有所不同）：

```
rpm -ivh kernel-hugemem-2.4.21-1.1931.2.399.ent.i686.rpm
```

- 如果你打算升级 kernel-source 或 kernel-utils 软件包，你可能不需要保留老版本。使用下面的命令来升级这些软件包（版本会有所不同）：

```
rpm -Uvh kernel-source-2.4.21-1.1931.2.399.ent.<arch>.rpm

rpm -Uvh kernel-utils-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

- 下一步是校验初始 RAM 磁盘映像是否被创建。

3.23.5 校验初始 RAM 磁盘映像

如果系统使用 ext3 文件系统或 SCSI 控制器，或使用标签来引用 /etc/fstab 中的分区，你就需要一个初始 RAM 磁盘。初始 RAM 磁盘允许模块化的内核在它能够进入模块通常驻留的设备之前具备进入内核需要从该设备引导的模块的能力。

在 IBM eServer iSeres 以外的 GTES10 体系上，初始 RAM 磁盘可以使用 mkinitrd 命令来创建。然而，如果内核及其相关文件是从 Turbolinux, Inc. 发行的 RPM 软件包中安装或升级的话，这个步骤就不必被手工进行。要校验它是否被创建了，使用 ls -l /boot 命令来确定 initrd-<version>.img 文件被创建了（版本应该匹配刚刚安装了的内核的版本）。

在 iSeries 系统上，初始 RAM 磁盘文件和 vmlinux 文件被合并成一个文件，它使用 mkinitrd 命令而被创建。如果内核及其相关文件是从 Turbolinux, Inc. 发行的 RPM 软件包中安装或升级的话，这个步骤会被自动执行；因此，它不必被手工进行。要校验它是否被创建了，使用 ls -l /boot 命令来确定 /boot/vmlinitrd-<kernel-version> 文件被创建了（版本应该匹配刚刚安装了的内核的版本）。

3.23.6 校验引导装载程序

kernel RPM 软件包配置引导装载程序来引导刚刚安装的内核（除了 IBM eServer iSeries 系统以外），但是它并不配置引导装载程序默认引导新内核。

确认一下引导装载程序已被配置成引导新内核总是值得提倡的。这是至关重要的一步。如果引导装载程序被配置得不正确，系统就不会正确引导 GTES10。若这种情况发生了，使用你从前创建的引导盘来引导你的系统，然后再试图配置你的引导装载程序。

3.23.6.1 x86 系统

x86 系统可以使用 GRUB 或 LILO 作为引导装载程序。只有一个例外—AMD64 系统不能使用 LILO。所有 x86 系统的默认引导装载程序都是 GRUB。

3.23.6.1.1 GRUB

如果你选择了 GRUB 作为引导装载程序，请确认 /boot/grub/grub.conf 文件中包含的 title 部分与你刚刚安装的 kernel 软件包的版本相同（如果你安装了 kernel-smp 或 kernel-bigmem 软件包，它们也会有各自的部分）：

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
```

```
#           all kernel and initrd paths are relative to /boot/, eg.
#           root (hd0,0)
#           kernel /vmlinuz-version ro root=/dev/hda2
#           initrd /initrd-version.img
#boot=/dev/hda
default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title GTES10 (2.4.21-1.1931.2.399.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-1.1931.2.399.ent ro root=LABEL=/
        initrd /initrd-2.4.21-1.1931.2.399.ent.img
title GTES10 (2.4.20-2.30.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.30.ent ro root=LABEL=/
        initrd /initrd-2.4.20-2.30.ent.img
```

如果你创建了单独的 /boot/ 分区，到内核与 initrd 映像的路径是相对于 /boot/ 分区而言的。

注意，默认引导项目没有被设置为新内核。要配置 GRUB 来默认引导新内核，把 default 变量的值改成包含新内核的 title 部分的号码。这个号码从 0 开始。例如，如果新内核是第一个 title 部分，把 default 设置为 0。

你可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

3.23.6.1.2 LILO

如果你选择了 LILO 作为引导装载程序，请确认 /etc/lilo.conf 文件中包含

的 image 部分与你刚刚安装的 kernel 软件包的版本相同（如果你安装了 kernel-smp 或 kernel-bigmem 软件包，它们也会有各自的部分）：

注意，默认引导项目没有被设置为新内核。要配置 LILO 来默认引导新内核，把 default 变量的值改成包含新内核的 image 部分中的 label 的值。以根用户身份运行 /sbin/lilo 命令来启用改变。运行后，其输出会与如下相似：

```
Added 2.4.21-1.1931.2.399.ent *

Added linux
```

2.4.21-1.1931.2.399.ent 后面的 * 意味着那部分中的内核是 LILO 会默认引导的内核。

你可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

3.23.6.2 Itanium 系统

Itanium 系统使用 ELILO 作为引导装载程序，该程序使用 /boot/efi/EFI/turbolinux/elilo.conf 作为配置文件。请确认该文件中包含的 image 部分与你刚刚安装的 kernel 软件包的版本相同：

```
prompt

timeout=50

default=old

image=vmlinuz-2.4.21-1.1931.2.399.ent

        label=linux

        initrd=initrd-2.4.21-1.1931.2.399.ent.img

        read-only

        append="root=LABEL=/"

image=vmlinuz-2.4.20-2.30.ent
```

```
        label=old
        initrd=initrd-2.4.20-2.30.ent.img
        read-only
        append="root=LABEL=/"
```

可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

3.23.6.3 IBM S/390 和 IBM eServer zSeries 系统

IBM S/390 和 IBM eServer zSeries 系统使用 z/IPL 作为引导装载程序。该程序使用 /etc/zipl.conf 作为配置文件。请确认该文件中包含一个带有和刚安装的内核版本相同的版本部分：

```
[defaultboot]
default=old
target=/boot/
[linux]
        image=/boot/vmlinuz-2.4.21-1.1931.2.399.ent
        ramdisk=/boot/initrd-2.4.21-1.1931.2.399.ent.img
        parameters="root=LABEL=/"
[old]
        image=/boot/vmlinuz-2.4.20-2.30.ent
        ramdisk=/boot/initrd-2.4.20-2.30.ent.img
        parameters="root=LABEL=/"
```

注意，默认引导项目没有被设置为新内核。要配置 z/IPL 来默认引导新内核，把 default 变量的值改成包含新内核部分的名称。每个部分的第一行在括号内包含名称。

修改了配置文件后，作为根用户运行以下命令来启用改变：

```
/sbin/zipl
```

你可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

3.23.6.4 IBM eServer iSeries 系统

/boot/vmlinitrd-<kernel-version> 文件在你升级内核的时候被安装。不过，你必须使用 dd 命令配置系统来引导新内核：

作为根用户，使用 cat /proc/iSeries/mf/side 命令来判定默认的边（A、B、或 C）。

作为根用户，使用以下命令（这里的 <kernel-version> 是新内核的版本，<side> 是前一个命令返回的边）：

```
dd if=/boot/vmlinitrd-<kernel-version> of=/proc/iSeries/mf/ \
<side>/vmlinux bs=8k
```

你可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

3.23.6.5 IBM eServer pSeries 系统

IBM eServer pSeries 系统使用 YABOOT 作为引导装载程序，该程序使用 /etc/aboot.conf 作为配置文件。请确认该文件包含的 image 部分和刚刚安装的 kernel 软件包是同一版本：

```
boot=/dev/sda1
init-message=Welcome to GTES10!
Hit <TAB> for boot options
partition=2
timeout=30
install=/usr/lib/yaboot/yaboot
```

```
delay=10
nonvram
image=/vmlinux--2.4.20-2.30.ent
        label=old
        read-only
        initrd=/initrd--2.4.20-2.30.ent.img
        append="root=LABEL=/"
image=/vmlinux-2.4.21-1.1931.2.399.ent
        label=linux
        read-only
        initrd=/initrd-2.4.21-1.1931.2.399.ent.img
        append="root=LABEL=/"
```

默认引导项目没有被设置为新内核。在第一个映像中的内核被默认引导。要把默认引导的内核该成新内核，把新内核的映像实例移到列表首位，或添加一个 default 指令，并把这个指令设置 为包含新内核的映像实例的 label。

可以重新引导计算机来开始测试这个新内核，观察屏幕上的消息来确保硬件被正确地检测到了。

3.24 内核模块

Linux 内核具有模块化设计。在引导时，只有少量的驻留内核被载入内存。这之后，无论何时用户要求使用驻留内核中没有的功能，某内核模块（kernel module），有时又称驱动程序（driver）。就会被动态地载入内存。

在安装过程中，系统上的硬件会被探测。基于探测结果和用户提供的信息，安装程序会决定哪些模块需要在引导时被载入。安装程序会设置动态载入机制来透明地运行。

如果安装后添加了新硬件，而这个硬件需要一个内核模块，系统必须被配置来为新硬件载入正确的内核模块。当系统使用新硬件引导后，Kudzu 程序会运行，如果新硬件被支持，它就会被检测到，该程序还会为它配置模块。你也可以通过编辑模块配置文件 /etc/modules.conf 来手工指定这个模块。

例如，如果某系统包括了一个 SMC EtherPower 10 PCI 网卡，模块配置文件包含以下行：

```
alias eth0 tulip
```

如果系统上添加了第二个网卡，它和第一个网卡一模一样，在 /etc/modules.conf 中添加这一行：

```
alias eth1 tulip
```

3.24.1 内核模块工具

如果安装了 modutils 软件包，你还可以使用一组管理内核模块的命令。使用这些命令来判定模块是否被成功地载入了，或为一件新硬件试验不同的模块。

/sbin/lsmod 命令显示了当前载入了的模块列表。例如：

```
 Module                   Size  Used by    Not tainted
iptable_filter            2412  0 (autoclean) (unused)
ip_tables                15864  1 [iptable_filter]
nfs                      84632  1 (autoclean)
lockd                    59536  1 (autoclean) [nfs]
sunrpc                   87452  1 (autoclean) [nfs lockd]
soundcore                 7044  0 (autoclean)
ide-cd                   35836  0 (autoclean)
cdrom                    34144  0 (autoclean) [ide-cd]
```

```
parport_pc             19204   1 (autoclean)
lp                      9188   0 (autoclean)
parport                39072   1 (autoclean) [parport_pc lp]
autofs                 13692   0 (autoclean) (unused)
e100                   62148   1
microcode               5184   0 (autoclean)
keybdev                 2976   0 (unused)
mousedev                5656   1
hid                    22308   0 (unused)
input                   6208   0 [keybdev mousedev hid]
usb-uhci               27468   0 (unused)
usbcore                82752   1 [hid usb-uhci]
ext3                   91464   2
jbd                    56336   2 [ext3]
```

对每行而言，第一列是模块名称；第二列是模块大小；第三列是用量计数。

用量计数后面的信息对每个模块而言都有所不同。如果 (unused) 被列在某模块的那行中，该模块当前就没在使用。如果 (autoclean) 被列在某模块的那行中，该模块可以被 rmmod -a 命令自动清洗。当这个命令被执行后，所有自从上次被自动清洗后未被使用的被标记了“autoclean”的模块都会被卸载。GTES10 不默认执行自动清洗行动。

如果模块名称被列举在行尾的括号内，括号内的模块就依赖于列举在这一行的第一列中的模块。例如，在以下行中：

```
usbcore                82752   1 [hid usb-uhci]
```

hid 和 usb-uhci 内核模块依赖于 usbcore 模块。

/sbin/lsmod 输出和查看 /proc/modules 的输出相同。

要载入内核模块，使用 /sbin/modprobe 命令，然后跟着内核模块的名称。

按照默认设置，modprobe 试图从 /lib/modules/<kernel-version>/kernel/drivers/ 子目录中载入模块。每类模块都有一个子目录，如用于网络接口驱动程序的 net/ 子目录。某些内核模块有模块依赖关系，这意味着你必须首先载入其它模块才能载入这些模块。 /sbin/modprobe 命令检查这些依赖关系，并在载入指定模块前载入满足这些依赖关系的模块。

例如：

```
/sbin/modprobe hid
```

这个命令载入任何满足依赖关系的模块，然后再载入 hid 模块。

要在 /sbin/modprobe 执行命令的时候把它们都显示在屏幕上，使用 -v 选项。例如：

```
 /sbin/modprobe -v hid
```

所显示的输出和下面相似：

```
/sbin/insmod
/lib/modules/2.4.21-1.1931.2.399.ent/kernel/drivers/usb/hid.o
Using
/lib/modules/2.4.21-1.1931.2.399.ent/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

你还可以使用 /sbin/insmod 命令来载入内核模块；不过它不解决依赖关系。因此，推荐你使用 /sbin/modprobe 命令。

要卸载内核模块，使用 /sbin/rmmod 命令和模块名称。rmmod 工具只卸载不在使用的、和不是被正使用的模块所依赖的模块。

例如：

```
/sbin/rmmod hid
```

这个命令卸载 hid 内核模块。

另一个有用的模块工具是 modinfo。使用 /sbin/modinfo 命令来显示内核模块的信息。一般语法是：

```
/sbin/modinfo [options] <module>
```

包括 -d 在内的选项显示了模块的简短描述，-p 选项列举了模块所支持的参数。

3.25 邮件传输代理（MTA）配置

邮件传输代理（Mail Transport Agent，MTA）是发送邮件的必备程序。邮件用户代理（Mail User Agent，MUA），如 Evolution、Mozilla Mail、Mutt，被用来阅读和编写电子邮件。当用户从 MUA 中发送一份邮件时，该邮件会被送到 MTA，然后 MTA 再把这份邮件发送给一系列 MTA，直到它到达最终发送目标为止。

即便用户不打算从系统中发送电子邮件，有些自动化的任务或系统程序可能仍会使用 /bin/mail 命令来把包含日志消息的邮件发送给本地系统的根用户。

GTES10 提供了两个 MTA：Sendmail 和 Postfix。如果两者均安装了，sendmail 就是默认的 MTA。邮件传输代理切换器允许用户选择 sendmail 或 postfix 作为系统的默认 MTA。

要使用基于文本的邮件传输代理切换器程序，你的系统上必须安装 system-switch-mail RPM 软件包。如果你想使用图形化版本，则 system-switch-mail-gnome 软件包也需要被安装。

要启动 邮件传输代理切换器，选择面板上的“主菜单 —> 系统工具 —> 邮件传输代理切换器”，或在 shell 提示（如 XTerm 或 GNOME 终端）中键入 system-switch-mail 命令。

该程序会自动检测 X 窗口系统是否在运行。如果它在运行，该程序就会在图形化模式中启动，如图 3–72 所示。如果没有检测到 X，它就会在文本模式中启动。要强制邮件传输代理切换器在文本模式下运行，使用 system-switch-mail-nox 命令。

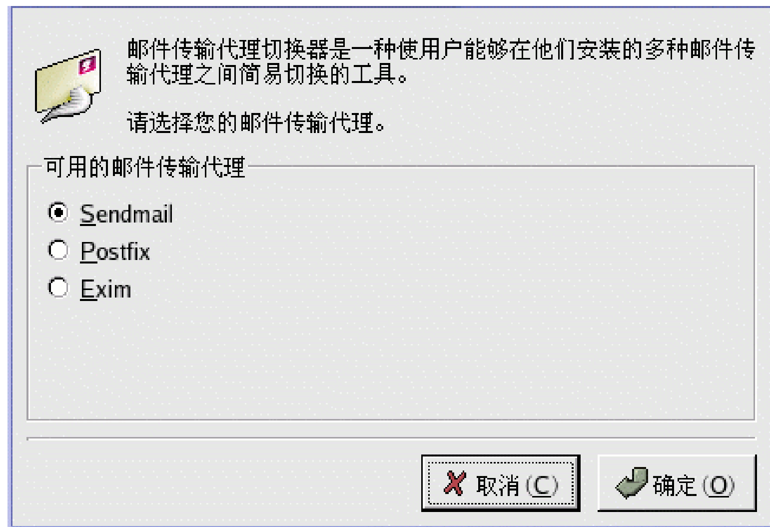


图 3-72 邮件传输代理切换器

如果你选择“确定”来改变 MTA，被选中的邮件守护进程就会在引导时被启动，未被选中的邮件守护进程会被禁用，这样，它就不会在引导时被启用；被选中的邮件守护进程被启动，其它邮件守护进程被停止，这样，改变就会立即发生。

3.26 系统监视

系统管理员还监视系统性能。TDS 包含协助系统管理员从事这些任务的工具。

3.26.1 收集系统信息

在你学习如何配置系统之前，你应该学习如何收集基本的系统信息。譬如，你应该知道如何找出空闲内存的数量、可用硬盘驱动器空间的数量，硬盘分区方案，以及正在运行进程的信息。本节将讨论如何使用几个简单程序来从你的 TDS 系统中检索这类信息。

3.26.1.1 系统进程

ps ax 命令显示一个当前系统进程的列表，该列表中包括其他用户拥有的进程。要显示进程以及它们的所有者，使用 ps aux 命令。该列表是一个静态列表；换一句话说，它是在你启用这项命令时正在运行的进程的快照。如果你需要一个时刻更新的运行进程列表，使用下面描述的 top 命令。

ps 的输出会很长。要防止它快速从屏幕中滑过，你可以把它管道输出给 less 命令：

```
ps aux | less
```

你可以使用 ps 命令和 grep 命令的组合来查看某进程是否在运行。譬如，要判定 Emacs 是否在运行，使用下面这个命令：

```
ps ax | grep emacs
```

top 命令显示了当前正运行的进程以及它们的重要信息，包括它们的内存和 CPU 用量。该列表既是真实时间的也是互动的。以下提供了一个 top 的输出示例：

```
19:11:04  up  7:25,  9 users,  load average: 0.00, 0.05, 0.12
89 processes: 88 sleeping, 1 running, 0 zombie, 0 stopped
CPU states:  cpu    user    nice   system    irq  softirq  iowait
idle
           total    6.6%    0.0%    0.0%   0.0%     0.0%    0.0%
192.8%
           cpu00    6.7%    0.0%    0.1%   0.1%     0.0%    0.0%
92.8%
           cpu01    0.0%    0.0%    0.0%   0.0%     0.0%    0.0%
100.0%
Mem:  1028556k av,  241972k used,  786584k free,       0k shrd,
37712k buff
```

```
      162316k active,             18076k inactive
Swap:  1020116k  av,               0k  used,  1020116k  free
99340k cached


  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME CPU
COMMAND
 1899 root      15   0 17728  12M  4172 S     6.5  1.2 111:20   0
X
 6380 root      15   0  1144 1144   884 R     0.3  0.1   0:00   0
top
    1 root      15   0   488  488   432 S     0.0  0.0   0:05   1
init
    2 root      RT   0     0    0     0 SW    0.0  0.0   0:00   0
migration/0
    3 root      RT   0     0    0     0 SW    0.0  0.0   0:00   1
migration/1
    4 root      15   0     0    0     0 SW    0.0  0.0   0:00   0
keventd
    5 root      34  19     0    0     0 SWN   0.0  0.0   0:00   0
ksoftirqd/0
    6 root      34  19     0    0     0 SWN   0.0  0.0   0:00   1
ksoftirqd/1
    9 root      25   0     0    0     0 SW    0.0  0.0   0:00   0
bdflush
    7 root      15   0     0    0     0 SW    0.0  0.0   0:00   1
kswapd
    8 root      15   0     0    0     0 SW    0.0  0.0   0:00   1
kscand
```

```
   10 root      15   0     0    0     0 SW     0.0  0.0   0:01   1
kupdated

   11 root      25   0     0    0     0 SW     0.0  0.0   0:00   0
mdrecoveryd
```

要退出 top，按 [q] 键。

可以和 top 一起使用的互动命令包括：

命令	描述
[Space]	立即刷新显示
[h]	显示帮助屏幕
[k]	杀死某进程。你会被提示输入进程 ID 以及要发送给它的信号。
[n]	改变要显示的进程数量。你会被提示输入数量。
[u]	按用户排序。
[M]	按内存用量排序。
[P]	按 CPU 用量排序。

表 3-6 互动的 top 命令

如果和 top 相比，你更喜欢使用图形化界面，你可以使用 GNOME 系统监视器。要从桌面上启动它，选择面板上的“主菜单 —> 系统工具 —> 系统监视器”或在 X 窗口系统的 shell 提示下键入 gnome-system-monitor。然后选择“进程列表”标签。

GNOME 系统监视器允许你在正运行的进程列表中搜索进程，还可以查看所有进程、你拥有的进程、或活跃的进程。

要了解更多某进程的情况，选择该进程，然后点击“更多信息”按钮。该进程的细节就会显示在窗口的底部。

要停止某进程，选择该进程，然后点击“结束进程”。这有助于结束对用户输入已不再做出反应的进程。

要按指定列的信息来排序，点击该列的名称。信息被排序的那一列会用深灰色显示。

按照默认设置，GNOME 系统监控器不显示线程。要改变这个首选项，选择“编辑 —> 首选项”，点击“进程列表”标签，然后选择“显示线程”。首选项还允许你配置更新间隔；每个进程默认显示的信息；以及系统监视器图表的颜色。



图 3-73 GNOME 系统监视器

3.26.1.2 内存用量

free 命令显示系统的物理内存和交换区的总量，以及已使用的、空闲的、共享的、在内核缓冲内的、和被缓存的内存数量。

```
             total       used       free     shared    buffers
cached
Mem:        256812     240668      16144     105176      50520
81848
-/+ buffers/cache:     108300     148512
Swap:       265032        780     264252
```

free -m 命令显示的信息和前面相同，但是它以 MB 为单位，便于阅读。

```
             total       used       free     shared    buffers
cached
Mem:           250        235         15        102         49
79
-/+ buffers/cache:        105        145
Swap:          258          0        258
```

如果和 free 相比，你更喜欢使用图形化界面，你可以使用 GNOME 系统监视器。要从桌面上启动它，选择面板上的“主菜单 —> 系统工具 —> 系统监视器”或在 X 窗口系统的 shell 提示下键入 gnome-system-monitor。然后选择“进程列表”标签。

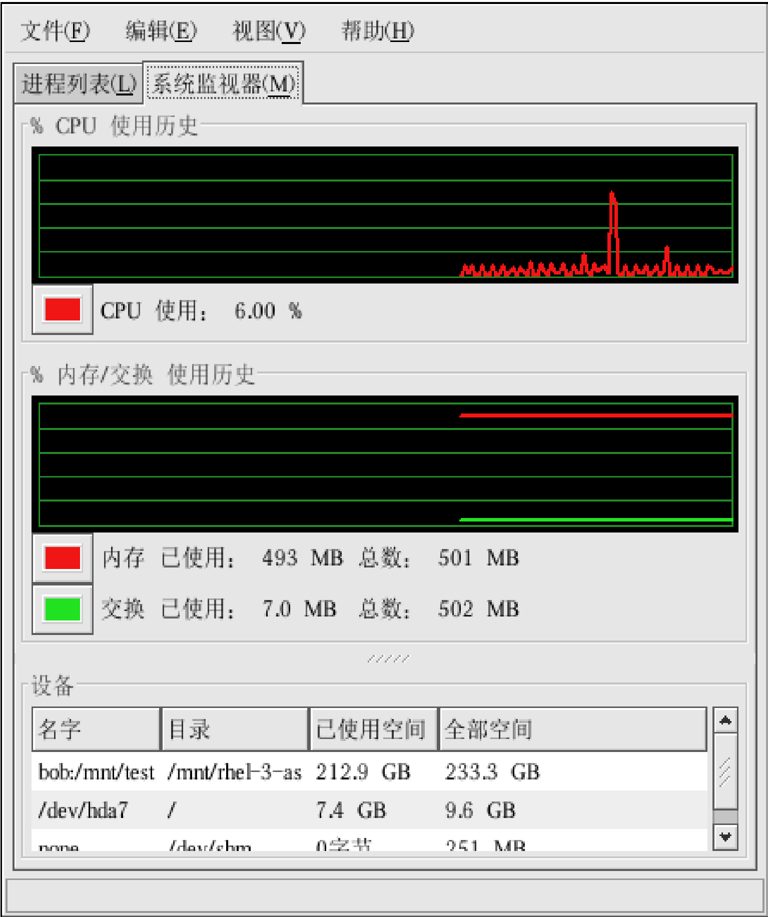


图 3-74 GNOME 系统监视器

3.26.1.3 文件系统

df 命令报告系统的磁盘空间用量。如果你在 shell 提示下键入了 df 命令，它的输出与下面相似：

```
Filesystem            1k-blocks      Used Available Use% Mounted on
/dev/hda2              10325716   2902060   6899140  30% /
```

```
/dev/hda1                15554      8656      6095  59% /boot
/dev/hda3             20722644   2664256  17005732  14% /home
none                    256796         0    256796   0% /dev/shm
```

按照默认设置，该工具把分区大小显示为 1KB 的块，已用的和可用的磁盘空间以 KB 为单位显示。要查看以 MB 和 GB 为单位的信息，使用 df -h 命令。-h 选项代表人可读格式。它的输出类似于：

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda2             9.8G  2.8G  6.5G  30% /
/dev/hda1              15M  8.5M  5.9M  59% /boot
/dev/hda3              20G  2.6G   16G  14% /home
none                  251M     0  250M   0% /dev/shm
```

在分区列表中，有一项是 /dev/shm。该项目代表系统的虚拟内存文件系统。

du 命令显示被目录中的文件使用的估计空间数量。如果你在 shell 提示下键入了 du 命令，每个子目录的用量都会在列表中显示，当前目录和子目录的总和也会在列表的最后一行中被显示。如果你不想查看每个子目录的用量，使用 du -hs 命令来使用人可读的格式只列出目录用量总和。使用 du --help 命令来查看更多选项。

要查看图形化的系统分区和磁盘空间用量，使用“系统监视器”标签。

3.26.1.4 硬件

如果你在配置硬件时遇到问题，或者只是想了解一下你的系统中有哪些硬件，你可以使用硬件浏览器 程序来显示能被探测到的硬件。要在桌面环境下启动该程序，点击“主菜单 —> 系统工具 —> 硬件浏览器”，或在 shell 提示下键入 hwbrowser。如图 3-75 所示，它显示了你的光盘设备、软盘、硬盘驱动器和它们的分区、网络设备、指示设备、系统设备、以及视频卡。点击左侧菜单上的类别名称，有关信息就会被显示。

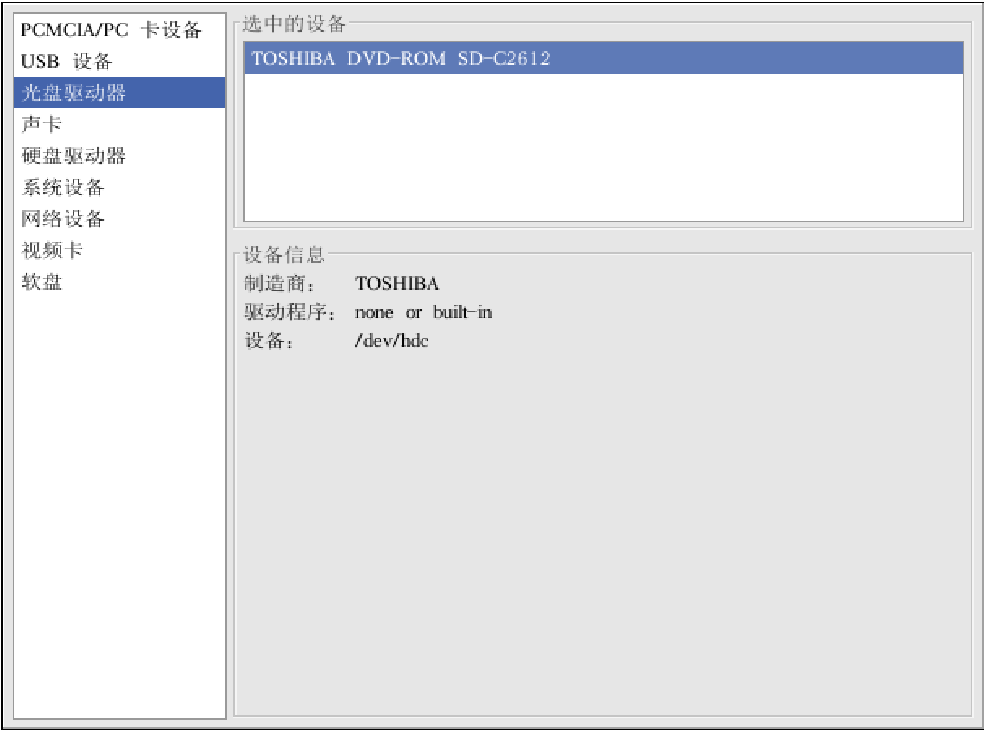


图 3-75 硬件浏览器

你还可以使用 lspci 命令来列举所有的 PCI 设备。使用 lspci -v 命令来获得详细的信息，或使用 lspci -vv 命令来获得更详细的输出。

譬如，lspci 命令可以被用来判定系统视频卡的制造厂商、型号、以及内存大小：

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400
AGP (rev 04) \

(prog-if 00 [VGA])

Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max

Flags: medium devsel, IRQ 16

Memory at f4000000 (32-bit, prefetchable) [size=32M]
```

```
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

如果你不知道系统网卡的制造商或型号，lspci 可以帮助你来判定这些信息。

3.26.2 OProfile

OProfile 是一个低管理费用的系统全局的性能监视工具。它使用处理器上的性能监视硬件来检索内核以及系统上的可执行文件的信息，例如内存是何时被引用的；L2 缓存请求数量；收到的硬件中断数量等。在 TDS 系统上，你必须安装 oprofile RPM 软件包才能使用该工具。

许多处理器都包含专用的性能监视硬件。该硬件能够在某些事件发生时（如所请求的数据不在缓存内）检测到它们。硬件通常是一个或多个计数器（counters），它们在每次事件发生时都递增一位。当计数器的值“翻转还原”，中断就会生成，从而能够控制性能监视的详细程度（以及由此带来的费用）。

OProfile 使用这个硬件（若没有性能监视硬件则使用一个基于计时器的代用品）来在每次计数器生成中断时收集与性能相关的数据样品（samples）。这些样品被定期写入磁盘；稍后，其中的数据就会被用来生成系统级别和应用程序级别的性能报告。

OProfile 是一个很有用的工具，但是请了解使用它的一些局限性：

- 对共享库的使用 — 除非使用 --separate=library 选项，共享库中的编码样品不会成为某个特定应用程序的属性。

- 性能监视样品不精确 — 当性能监视注册器引发了抽样行动，中断处理将不会明确给出例外的类型。由于处理器要无序地执行指令，样品可能

会在附近的指令上被抽取。

• oprofpp 不能够正确地归类内联函数样品 — oprofpp 使用一个简单的地址范围机制来决定它所在的是哪个函数的地址。内联函数样品不从属于那个内联函数，而是从属于那个内联函数所插入的函数。

• OProfile 从多次运行中积累数据 — OProfile 是一个系统范围内的建档器，它预计进程会被多次启动和关闭。这样，样品就会从多次运行实例中被积累下来。使用 opcontrol --reset 来清除从以前运行实例中抽取的样品。

• 非 CPU 约束的性能问题 — OProfile 能够找出受 CPU 约束的进程的问题。OProfile 不会识别正处于睡眠状态的进程，因为这些进程正在等待锁或其它事件的发生（如等待 I/O 设备完成操作）。

在 TDS 中，只有多处理器（SMP）内核才启用了 OProfile 支持。要判定运行的是哪个内核，使用以下命令：

```
Uname –r
```

如果返回的内核版本以 .entsmp 结束，运行的就是多处理器内核。否则，即使系统不是多处理器系统，也请通过网络或发行光盘来安装它。多处理器内核可以在单处理器内核上运行。

3.26.2.1 工具总览

表 3-7 提供了对 oprofile 软件包中包括的工具的总览。

命令	描述
opcontrol	配置要收集的数据。
op_help	显示系统处理器的可用事件以及每个事件的简单描述。
op_merge	合并同一可执行文件的多个样品。
op_time	提供对所有建档的可执行文件的总览。
op_to_source	如果应用程序使用调试符号编译了，创建带注解的源码。

oprofiled	作为守护进程来运行，定期把样品数据写入磁盘。
oprofpp	检索档案数据。
op_import	把样品数据库文件从异类二进制格式转换成系统的本地原始格式。只有在分析不同体系的样品数据库时才使用该选项。

表 3-7 OProfile 命令

3.26.2.2 配置 OProfile

在运行 OProfile 之前，它必须被配置。至少需要选择是否要监视内核。以下各节描述了如何使用 opcontrol 工具来配置 OProfile。在 opcontrol 命令被执行时，设置选项就会被保存到 /root/.oprofile/daemonrc 文件中。

3.26.2.2.1 指定内核

首先，配置 OProfile 是否应该监视内核。这是在启动 OProfile 前唯一所需的配置选项。其它选项都是可选的。

要监视内核，以根用户身份执行以下命令：

```
opcontrol --vmlinux=/boot/vmlinux-`uname -r`
```

要配置 OProfile 不监视内核，以根用户身份执行以下命令：

```
opcontrol --no-vmlinux
```

这个命令还会载入 oprofile 内核模块（如果还没有被载入），并创建 /dev/oprofile/ 目录（如果不存在）。

设置样品是否应在内核中收集只会改变所收集的数据，而不会改变收集数据的方法或贮存地点。

3.26.2.2.2 设置要监视的事件

多数处理器包含计数器（counters）。它们被 OProfile 用来监视指定的事件。

如表 3-8 所示，可用的计数器的数量要根据处理器而定。

处理器	Cpu 类型	计数器数量
Pentium Pro	i386/ppro	2
Pentium II	i386/pii	2
Pentium III	i386/piii	2
Pentium 4（无超线程）	i386/p4	8
Pentium 4（有超线程）	i386/p4-ht	4
Athlon	i386/athlon	4
AMD64	x86-64/hammer	4
Itanium	ia64/itanium	4
Itanium 2	ia64/itanium2	4
TIMER_INT	计时器（timer）	1
IBM eServer iSeries	计时器（timer）	1
IBM eServer pSeries	计时器（timer）	1
IBM eServer S/390	计时器（timer）	1
IBM eServer zSeries	计时器（timer）	1

表 3-8. OProfile 处理器和计数器

使用表 3-8 的信息来校验所检测到的处理器类型是否正确，并且判定能够被同时监视的事件数量。如果处理器没有支持的性能监视硬件，计时器（timer）就会被用作处理器类型。

如果使用了 timer，事件就不能为任何处理器设置，因为硬件不支持硬件性能计数器。相反，计时器中断会被用来建档。

如果 timer 没有被用作处理器类型，监视的事件就可以被改变，处理器的计数器 0 就会被默认设置为基于时间的事件。如果处理器上有多个计数器，0 以外的计数器就不会被默认设置任何事件。被监视的默认事件显示在表 3-9 中。

处理器	计数器 0 的默认事件	描述
Pentium Pro, Pentium II, Pentium III, Athlon, AMD64	CPU_CLK_UNHALTED	处理器的时钟没有停止
Pentium 4 (HT 和非 HT)	GLOBAL_POWER_EVENTS	处理器没有停止的时间
Itanium 2	CPU_CYCLES	CPU 周期
TIMER_INT	(none)	每个计时器中断的抽样

表 3-9 默认事件

可以被同时监视的事件数量是由处理器的计数器数量决定的。不过，这不是一对一的情况；在某些处理器上，某些事件必须被映射到指定的计数器上。要判定可用的计数器数量，执行以下命令：

```
cat /dev/oprofile/cpu_type
```

可用的事件要根据处理器类型而定。要判定可被建档的事件，以根用户身份执行以下命令（该列表是针对系统处理器类型特有的）：

```
op_help
```

每个计数器的事件都可以通过命令行被配置，也可以使用图形化界面配置。如果计数器没有被设置给指定的事件，错误消息就会被显示。

要通过命令行来为每个可配置的计数器设置事件，使用 opcontrol：

```
opcontrol --ctrlN-event=<event-name>
```

把 N 替换成计数器号码(从0开始),把 <event-name> 替换成 op_help 中显示的确切事件名称。

- 抽样率

默认设置会选择基于时间的事件设置。它大约会创建每处理器每秒 2000 个样品。如果使用了计时器中断，计时器就被设置成两幅画面的最小时间

间隔率，而且还不能被用户设置。如果 cpu_type 不是 timer，每个事件就必须设置了一个抽样率（sampling rate）。抽样率是每次抽样之间发生的事件数量。

在为计数器设置事件时，还可以指定一个抽样率：

```
opcontrol --ctrN-event=<event-name> --ctrN-count=<sample-rate>
```

把 <sample-rate> 替换成再次抽样前要等待的事件数量。这个值越小，抽样的频率就越高。对于不常发生的事件，你可能需要使用一个较小的值才能捕获事件实例。

- 单元屏蔽

如果 cpu_type 不是 timer，那么就可能还需要单元屏蔽（unit masks）来进一步确定事件。

每个事件的单元屏蔽可以使用 op_help 命令列举。每个单元屏蔽的值都以十六进制格式显示。要指定一个以上单元屏蔽，十六进制的值必须使用逐位"或"（or）算符来组合。

```
opcontrol  --ctrN-event=<event-name>  --ctrN-count=<sample-rate>
--ctrN-unit-mask=<value>
```

3.26.2.2.3 分离内核和用户空间档案

按照默认设置，每个事件都收集内核模式和用户模式的信息。要配置 OProfile 在某个指定的计数器中不计数内核模式的事件，执行以下命令（这里的 N 是计数器号码）：

```
opcontrol --ctrN-kernel=0
```

执行以下命令来再次启动计数器的建档内核模式：

```
opcontrol --ctrN-kernel=1
```

要配置 OProfile 不计数某个指定计数器的用户模式的事件，执行以下命令（这里的 N 是计数器号码）：

```
opcontrol --ctrN-user=0
```

执行以下命令来再次启动计数器的建档用户模式：

```
opcontrol --ctrN-user=1
```

当 OProfile 守护进程把档案数据写入样品文件，它可以把内核和库档案的数据分成两个单独的样品文件。要配置守护进程写入样品文件的方式，以根用户身份执行以下命令：

```
opcontrol --separate=<choice>
```

<choice> 可以是以下之一：

- none — 不要分离档案（默认）
- library — 为库生成每个应用程序的档案
- kernel — 为内核和内核模块生成每个应用程序的档案
- all — 为库生成每个应用程序的档案，为内核和内核模块生成每个应用程序的档案

如果 --separate=library 被使用，抽样文件名在包括可执行文件名称的同时还包括库的名称。

3.26.2.3 启动和停止 OProfile

要使用 OProfile 来开始监视系统，以根用户身份执行以下命令：

```
opcontrol --start
```

所显示的输出和下面相似：

```
Using log file /var/lib/oprofile/oprofiled.log

Daemon started.

Profiler running.
```

/root/.oprofile/daemonrc 中的设置被使用。

OProfile 守护进程 oprofiled 被启动；它定期把样品数据写入 /var/lib/oprofile/samples/ 目录。该守护进程的日志位于 /var/lib/oprofile/oprofiled.log。

如果 OProfile 使用不同的配置选项被重新启动，以前会话中的样品文件就会被自动备份到 /var/lib/oprofile/samples/session-N 目录中，这里的 N 是前一次备份会话数量再加 1。

```
Backing up samples file to directory /var/lib/oprofile/samples//session-1

Using log file /var/lib/oprofile/oprofiled.log

Daemon started.

Profiler running.
```

要停止建档器，以根用户身份执行以下命令：

```
opcontrol --shutdown
```

3.26.2.4 保存数据

有时，在指定时间保存样品会很有用。例如，在给可执行文件建档的时候，根据不同的输入数据来收集不同的样品可能会很有用。如果要监视的事件数量超过了处理器可用的计数器数量，你可以运行多次 OProfile 来收集数据，每次都把样品数据保存到不同的文件中。

要保存当前的抽样文件集合，执行以下命令，把 <name> 替换成当前会话中的独特描述性名称。

```
opcontrol --save=<name>
```

目录 /var/lib/oprofile/samples/name/ 被创建，当前的抽样文件被复制到其中。

3.26.2.5 分析数据

OProfile 守护进程 oprofiled 定期收集样品，并把它们写入 /var/lib/oprofile/samples/ 目录。在读取数据之前，请以根用户身份执行以下命令来确定所有数据都被写入这个目录中了：

```
opcontrol --dump
```

每个样品文件名称都基于可执行文件的名称，使用右括号（}）来代替每个正斜线（/）。文件名的结尾是井号（#）和用于该样品文件的计数器号码。例如，以下文件包括了计数器 0 所收集的 /sbin/syslogd 这个可执行文件的样品数据：

```
}sbin}syslogd#0
```

一旦抽样数据被收集，你可以使用以下工具来分析它们：

- op_time
- oprofpp
- op_to_source
- op_merge

使用这些工具以及被建档的二进制文件来生成可以进一步被分析的报告。

每个可执行文件的样品都被写入一个样品文件。每个动态链接库的样品也被写入一个样品文件。在 OProfile 运行的时候，如果被监视的可执行文件改变了，而且用于这个可执行文件的样品文件存在，这个现存的样品文件就会被自动删除。因此，如果这个样品文件要被保留，它就必须在可执行文件被新版本替代前和所用的可执行文件一起备份。

3.26.2.5.1 使用 op_time

op_time 提供了对所有建档的可执行文件的总览。

以下是输出示例的一部分：

```
581     0.2949  0.0000 /usr/bin/oprofiled
966     0.4904  0.0000 /usr/sbin/cupsd
1028    0.5218  0.0000 /usr/sbin/irqbalance
1187    0.6026  0.0000 /bin/bash
1480    0.7513  0.0000 /usr/bin/slocate
2039    1.0351  0.0000 /usr/lib/rpm/rpmq
```

```
6249        3.1722   0.0000 /usr/X11R6/bin/XFree86
8842        4.4885   0.0000 /bin/sed
31342      15.9103   0.0000 /usr/bin/gdmgreeter
58283      29.5865   0.0000 /no-vmlinux
82853      42.0591   0.0000 /usr/bin/perl
```

每个可执行文件都在它自己的行上列出。第一列是为该可执行文件记录的样品数量。第二列是样品和样品总数的百分比。第三列没有被使用，第四列是这个可执行文件的名称。

3.26.2.5.2 使用 oprofpp

要检索指定可执行文件的详细信息，使用 oprofpp：

```
oprofpp <mode> <executable>
```

<executable> 必须是到要分析的可执行文件的完整路径。<mode> 必须是以下之一：

- -l

按照符号列举样品数据。例如：以下是运行命令 oprofpp -l /usr/X11R6/bin/XFree86 的部分输出：

```
vma      samples  %          symbol name
...
08195d10 4        3.0303     miComputeCompositeClip
080b9180 5        3.78788    Dispatch
080cdce0 5        3.78788    FreeResource
080ce4a0 5        3.78788    LegalNewID
080ce640 5        3.78788    SecurityLookupIDByClass
080dd470 9        6.81818    WaitForSomething
080e1360 12       9.09091    StandardReadRequestFromClient
```

```
...
```

第一列是虚拟内存地址（vma）的起点。第二列是该符号的样品数量。第三列是该符号的样品和该可执行文件的总体样品的百分比。第四列是符号的名称。

要把输出按照样品的数量多少排序（反向），使用 -r 和 -l 选项。

- -s <symbol-name>

列举某个符号名称特有的样品数据。例如：以下输出是从命令 oprofpp -s StandardReadRequestFromClient /usr/X11R6/bin/XFree86 中截取的：

```
vma      samples  %          symbol name
080e1360 12       100        StandardReadRequestFromClient
080e1360 1        8.33333
080e137f 1        8.33333
080e13bb 1        8.33333
080e13f4 1        8.33333
080e13fb 1        8.33333
080e144a 1        8.33333
080e15aa 1        8.33333
080e1668 1        8.33333
080e1803 1        8.33333
080e1873 1        8.33333
080e190a 2        16.6667
```

第一行是符号/可执行文件组合的摘要。

第一列包括抽样的虚拟内存地址。第二列是该内存地址的抽样数量。第三列是该内存地址的样品和该符号的样品总数的百分比。

- -L

按照符号列举样品数据，比 -l 更详细。例如：

```
vma      samples  %          symbol name
08083630 2        1.51515    xf86Wakeup
 08083641 1        50
 080836a1 1        50
080b8150 1        0.757576   Ones
 080b8179 1        100
080b8fb0 2        1.51515    FlushClientCaches
 080b8fb9 1        50
 080b8fba 1        50
...
```

数据和 -l 选项一样，只不过，对于每个符号来说，每个所用的虚拟内存地址都被显示。对于每个虚拟内存地址，样品数量以及样品和该符号的样品数量的百分比也被显示。

- -g <file-name>

按照 gprof 格式把输出生成到文件中。如果生成的文件叫做 gmon.out，gprof 就能够被用来进一步分析数据。

能够进一步限定数据的其它选项如下：

- -f <file-name>

使用指定的样品文件 <file-name>。按照默认设置，/var/lib/oprofile/samples/ 中的样品文件会被使用。使用这个选项来指定来自前一个会话的样品文件。

- -i <file-name>

使用 <file-name> 作为要检索数据的可执行文件的名称。

- -d

给 C++ 符号名称解码（demangle）。

- -D

给 C++ 符号名称解码（demangle），简化 STL 库的解码名称。

- --counter <number>

为指定计数器收集信息。若没有指定，默认的计数器是 0。

- -o

每个样品都显示源码中的行号。当可执行文件被编译时，应该使用 GCC 的 -g 选项。否则，该选项将无法显示行号。TDS 的可执行文件默认都没有使用这个选项编译。

```
vma      samples  %      symbol name        linear info

0806cbb0       0                                        0
_start              ../sysdeps/i386/elf/start.S:47
```

- -e <symbol-name>

在输出中不包括用逗号分隔的符号列表。

- -k

显示包含共享库的附加列。这个选项只有在配置 OProfile 时指定了 --separate=library 选项，同时又没有指定 --dump-gprof-file 选项时才会生成结果。

- -t <format>

按照指定列顺序来显示输出。该选项不能和 -g 一起使用。

使用以下字母来代表列：

字母	描述
v	虚拟内存地址
s	样品数量
S	样品的累计数量
p	样品和该可执行文件的样品总数的相对百分比
P	样品和该可执行文件的样品总数的累计百分比

q	相对于所有抽样的可执行文件的样品百分比
Q	相对于所有抽样的可执行文件的样品累计百分比
n	符号名称
l	源文件的名称和行号，包括完整路径
L	源码文件名的基准名称和行号
i	可执行文件的名称，包括完整路径
I	可执行文件的基准名称
d	样品的细节
h	显示列标头

表 3-10 用字母代表列的顺序

- --session <name>

指定到会话的完整路径或相对于 /var/lib/oprofile/samples/ 目录的目录。

- -p <path-list>

指定要分析的可执行文件所在的用逗号分隔的路径列表。

3.26.2.5.3 使用 op_to_source

op_to_source 工具试图匹配特定指令的样品和源码中相对应的行。所生成的文件应该在左侧列出这些行的样品。它还会在每个函数的开头插入注释，列举该函数的样品总数。

要使用这个工具，可执行文件必须使用 GCC 的 -g 选项编译。TDS 软件包没有默认使用这个选项编译。

op_to_source 的一般语法是：

```
op_to_source --source-dir <src-dir> <executable>
```

必须指定包含要被分析的源码和可执行文件的目录。

3.26.2.5.4 使用 op_merge

如果存在多个用于同一可执行文件或库的样品文件，样品文件可以被合并来简化分析。

例如：要合并 /usr/lib/library-1.2.3.so 库的文件，以根用户身份运行以下命令：

```
op_merge /usr/lib/library-1.2.3.so
```

结果文件是 /var/lib/oprofile/samples/}usr}lib}library-1.2.3.so。

要限制样品文件被合并到指定的计数器，使用 -c 选项，再跟随一个计数器号码。

3.26.2.6 理解/dev/profile/文件

/dev/oprofile/ 目录包含 OProfile 的文件系统。使用 cat 命令来显示这个文件系统的虚拟文件值。例如：以下命令显示 OProfile 检测到的处理器类型：

```
cat /dev/oprofile/cpu_type
```

/dev/oprofile/ 中有用于每个计数器的目录。例如：如果计数器有两个，其中就会有 /dev/oprofile/0/ 和 dev/oprofile/1/ 这两个目录。

计数器的每个目录中都包含以下文件：

count — 抽样间隔

enabled — 如果是 0，计数器就被关闭，不会为它收集样品；如果是 1，计数器就被开启，样品就会为它收集。

event — 要监视的事件

kernel — 如果是 0，当处理器在内核空间时，样品就不会为这个计数器事件而收集；如果是 1，即便处理器在内核空间时，样品也会被收集。

unit_mask — 为计数器启用的是哪些单元屏蔽

user — 如果是 0，当处理器在用户空间时，样品就不会为计数器事件收集；如果是 1，即便处理器在用户空间时，样品也会被收集。

这些文件的值可以使用 cat 命令来检索。例如：

```
cat /dev/oprofile/0/count
```

3.26.2.7 用法示例

OProfile 不但能够被开发者用来分析应用程序的性能，它还能够被系统管理员用来进行系统性能分析。例如：

判定哪些应用程序和服务在系统上被使用得最多 — op_time 可以被用来判定应用程序或服务使用了多少处理器时间。如果系统被用于多种服务，但是却表现不佳，使用最多处理器时间的服务就可以被转移到专职系统上。

判定处理器用量 — CPU_CLK_UNHALTED 事件可以被监视，以便判定某段给定时间内的处理器载量。然后，这个数据就可以被用来判断另加一个处理器或更快的处理器是否会提高系统性能。

3.26.2.8 图形化界面

某些 OProfile 首选项可以使用图形化界面来设置。要启动它，在 shell 提示下以根用户身份执行 oprof_start 命令。

改变了选项后，点击 Save and quit 按钮来保存它们。首选项会被写入 /root/.oprofile/daemonrc，应用程序也会退出。退出该应用程序并不会停止 OProfile 的抽样进程。

在 Setup 活页标签上，从拉下菜单中选择计数器，从列表中选择事件。对事件的简单描述会出现在列表下面的文本箱内。只有用于指定计数器和指定体系的可用事件才会被显示。该界面还显示建档器是否在运行，以及简短的统计。

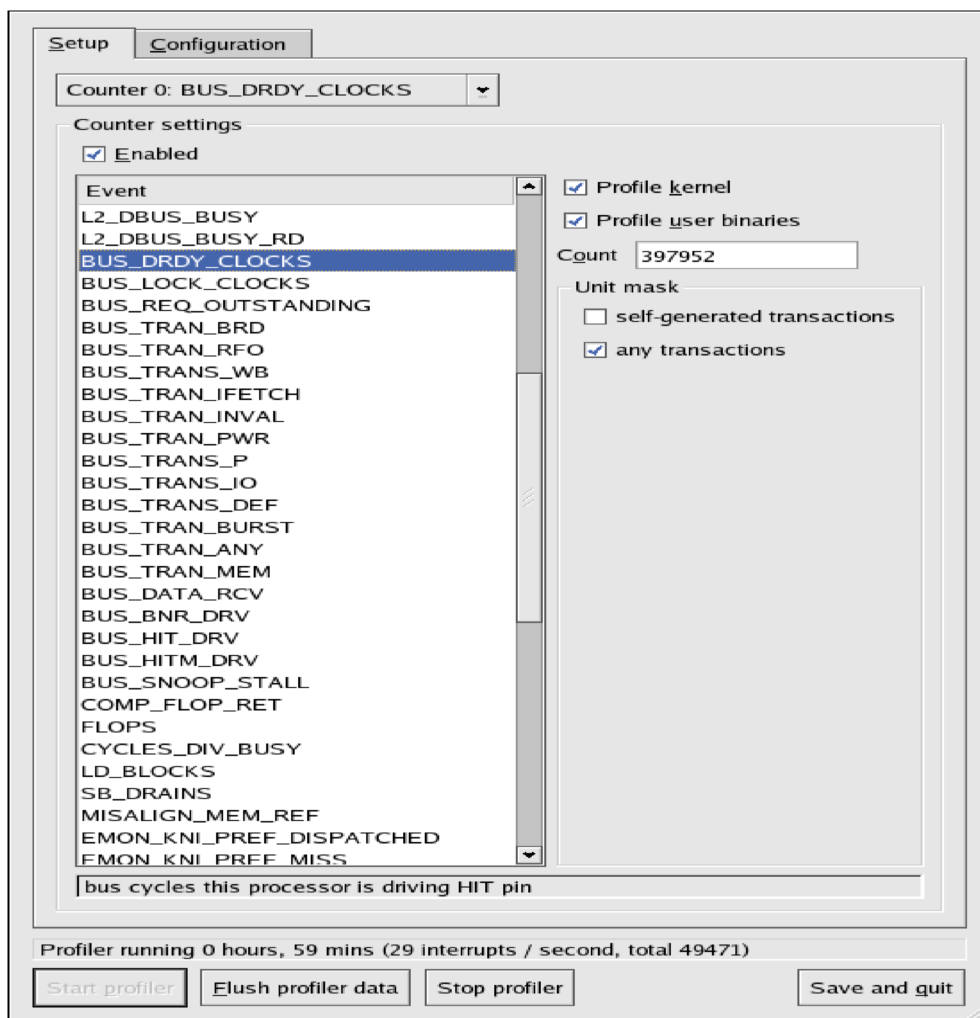


图 3-76 OProfile 设置

在活页标签的右侧，选择 Profile kernel 选项来为当前选定的事件计数内核模式中的事件。这和 opcontrol --ctrN-kernel=1 命令等同，这里的 N 是计数器号码。如果该选项没有被选，它就和 opcontrol --ctrN-kernel=0 命令等同。

选择 Profile user binaries 选项来为当前选定的事件计数用户模式中的事

件。这和 opcontrol --ctrN-user=1 命令等同，这里的 N 是计数器号码。如果该选项没有被选，它就和 opcontrol --ctrN-user=0 命令等同。

如果当前选择的事件中有可用的单元屏蔽，它们会被显示在 Setup 活页标签右侧的 Unit Masks 里面。选择单元屏蔽旁边的复选箱来为该事件启用它。

在 Configuration 活页标签上，要给内核建档，在 Kernel image file 文本字段中输入要监视的内核的 vmlinux 文件的名称和位置。要让 OProfile 不监视内核，选择 No kernel image。

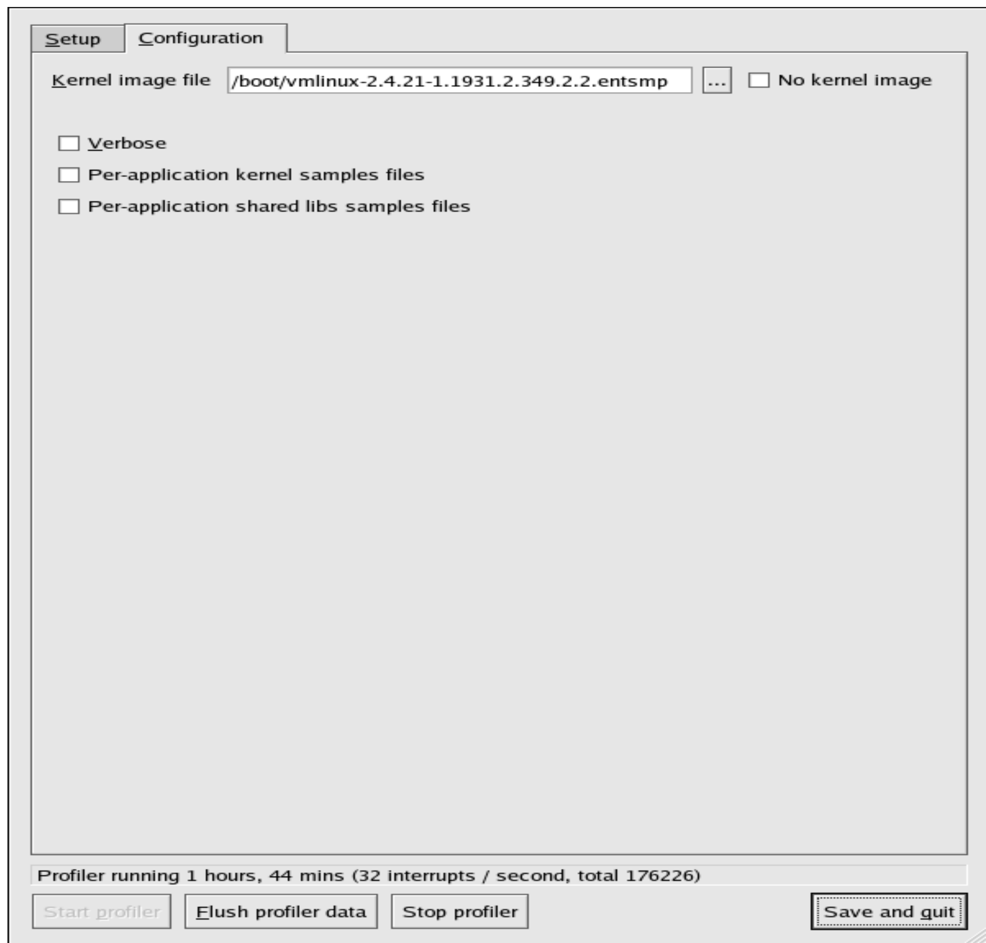


图 3-77 OProfile 配置

如果选择了 Verbose 选项，oprofiled 守护进程日志就会包括更多信息。

如果选择了 Per-application kernel samples files，OProfile 会为内核以及内核模块生成每应用程序的档案。这和 opcontrol --separate=kernel 命令等同。如果选择了 Per-application shared libs samples files，OProfile 为库生成每应用程序档案。这和 opcontrol --separate=library 命令等同。

要强制数据写入样品文件，点击 Flush profiler data 按钮。这和 opcontrol --dump 命令相等。

要从图形化界面启动 OProfile，点击 Start profiler。要停止建档器，点击 Stop profiler。退出程序并不会停止 OProfile 的抽样活动。

第四章　GTES10 安全指南

4.1 介绍

本章的目的是为 GTES10 用户学习提供服务器工作站的安全、防止入侵等的相关技术。本章详细地介绍了数据中心、工作和家庭等创建安全计算机环境所应采取的计划和工具。GTES10 能在系统功能和性能基本不受影响的情况下，提供可靠的网络安全功能。

4.1.1 体系特有的信息

除非另外说明，本书中的所有信息都只应用于 x86 处理器以及使用 Intel? Extended Memory 64 Technology (Intel® EM64T) 和 AMD64 技术的处理器。

4.2 安全概述

随着商业和个人对网络计算的依赖性的日益增强，许多网络和计算机安全相关的行业也渐渐形成。企业机构开始聘请安全专家来精确地评审系统以及定制适合其组织的解决方案。由于许多机构属于动态性质，工作人员可以以本地和远程的方式使用公司的信息资源，因此机构对安全计算环境的需求已愈来愈强烈。

然而，多数机构（以及个体用户）把安全问题当成"马后炮"。安全问题常常会被忽略。正确的安全措施经常是在事后调查（postmortem）后才被实施，即在非法入侵事件出现之后。安全专家一致认为，在把网站连接到不信任的网络（如国际互联网）之前预先采取正确的措施是防止入侵的有效方法。

4.2.1 什么是计算机安全

计算机安全这个术语所涉及的计算和信息处理领域比较广泛。对于依赖于计算机系统和网络来处理日常商业事务和存取重要信息的公司，数据是公司总资产的重要组成部分。一些术语和衡量标准也逐渐出现，例如：整体拥有成本（total cost of ownership，TCO）、服务质量（quality of service，QoS）。在这些衡量标准中，行业把数据完好性和高可用性方面也计算入他们的计划和进程管理费用中，在某些行业（如电子商务）中，数据的可用性和可信性是至关重要的。

4.2.1.1 计算机安全问题溯源

许多读者可能还会记得电影《战争游戏》。电影讲述了因为误入美国国防部超级电脑而无意中导致核战争危机的故事。电影的流行激发了许多个人和团体开始实施电影所描述的闯入机密系统的方法，包括著名的"战争拨号（war dialing）" —— 按照区号和电话前缀组合来搜索模拟调制解调器连接的电话号码。

十多年后，通过美国联邦调查局（FBI）和全美国的计算机专家的鼎力合作，以及历时四年的多司法区的追踪，声名狼藉的计算机怪客凯文 • 米蒂尼克（Kevin Mitnick）终于被逮捕。他被指控了 25 项计算机和存取设备的诈骗盗窃罪。这些诈骗盗窃活动导致诺基亚（Nokia）、NEC、Sun Microsystems、Novell、富士（Fujitsu）、和摩托罗拉（Motorola）损失了近八千万美元的知识产权和源码。该案件被 FBI 认为是当时美国历史上最大的计算机犯罪案件。凯文 • 米蒂尼克被定罪并被判处了 5 年零 8 个月的徒刑。他共服刑 5 年，于 2000 年 1 月 21 日被假释。假释条件禁止他在 2003 年之前使用计算机或从事任何和计算机相关的顾问工作。调查员说，米蒂尼克是社交工程（social engineering） —— 使用人际关系来获得口令，使用伪造身份来进入系统 —— 的专家。

随着对使用公共网络来传送私人、财经、以及其它保密信息的依赖性越来越大，信息安全的性质也越来越重要。米蒂尼克这类案件的层出不穷，使得各行各业都不得不开始重新考虑他们处理信息传输的策略。互联网的流行，使得数据安全被提上日程。

越来越多的人使用他们的个人计算机来获取互联网所提供的各项资源，从研究、信息检索，到电子邮件和电子商务。互联网已被公认为是二十世纪最重要的开发成果之一。

然而，互联网和它早期的协议都是基于信任（trust-based）系统。这就是说，互联网协议自身的设计是不安全的。TCP/IP 协议栈中没有内建任何进行审核的安全标准，因此带有潜在不良企图的网络用户和进程几乎能够畅行无阻。虽然当前的开发已大大提高了互联网通信的安全性，但没有绝对安全的系统和网络。

4.2.1.2 计算机安全大事表

在计算机安全问题的发生和发展过程中出现了几件对其深远影响的重要事件。以下列出了一些使人们开始关注计算机和信息安全的重要事件。

4.2.1.2.1 三十年代和四十年代

波兰密码破译家在 1918 年发明了 Enigma 机器。它是一个机械式螺旋密码计算设备。它把纯文本消息转换成加密文本。最初，这是为保护银行通信安全而开发的。在第二次世界大战时，德国军事部门发觉该设备具备加密通讯的潜力。一个叫做 Alan Turing 的卓越数学家发明了攻破 Enigma 密码的方法，从而使联军开发了叫做 Colossus 的机器。很多资料都认为 Colossus 使二战提前一年结束。

4.2.1.2.2 六十年代

麻省理工学院（MIT）的学生组织了技术模型铁路俱乐部（Tech Model Railroad Club，TMRC），开始使用学院里的 PDP-1 大型机进行编程探索。最终，这个小组发明了"黑客"这个术语，其意义和今天相仿。

美国国防部创建了高级研究计划局网（Advanced Research Projects Agency Network，ARPANet）。它在研究界和学术界越来越流行，逐渐成为电子数据信息的交换渠道。这为创建今天所称的"互联网"奠定了基础。

Ken Thompson 开发了 UNIX 操作系统。由于这个系统提供了使用方便的开发工具和编译器，以及支持性的用户社区，它被广泛认为是最"黑客友好"的操作系统。与此同时，Dennis Ritchie 开发了 C 编程语言，该语言可以说是计算机历史上最流行的黑客语言。

4.2.1.2.3 七十年代

Bolt, Beranek, and Newman 是美国政府和行业内的计算机研究和开发承包商。它们开发了 Telnet 协议 —— ARPANet 的公共扩展。该协议为公开使用从前仅限于政府承包商和学术研究者的数据网络打开了方便之门。据几位安全研究员表明，Telnet 也可以算是公共网络中最不安全的协议。

Steve Jobs 和 Steve Wozniak 创办了苹果计算机（Apple Computer），并开始推销个人计算机（PC）。PC 是一些蓄意不良的用户学习使用普通电脑通信硬件（如模拟调制解调器和战争拨号器）来远程入侵系统这门艺术的跳板。

Jim Ellis 和 Tom Truscott 创建了 USENET —— 用于在分散的用户间进行电子通信的公告板风格的系统。USENET 迅速成为交换计算、联网、以及入侵攻击方面的观点见解的最流行论坛之一。

4.2.1.2.4 八十年代

IBM 开发并销售基于 Intel 8086 微型处理器的 PC。它是一种相对来说价格较低廉的体系，它把计算机从办公室延伸到了家庭。它使 PC 渐渐成为一种功能比较强大、使用方便、而又普通常见、极易获取的工具，从而促进了这类硬件在恶意用户的家庭和办公场所日益增多。

由 Vint Cerf 开发的传输控制协议被分裂成两个独立的部分。互联网协议（IP）就是从这次分裂中诞生的。被组合在一起的 TCP/IP 协议成为今天所有互联网通信的标准。

基于在电话欺诈（phreaking） —— 探索和攻击电话系统 —— 方面的发展情况，2600: The Hacker Quarterly 杂志被创办。该杂志开始面向比较广泛的读者听众，讨论入侵计算机和计算机网络之类的课题。

经过九天的自由入侵，414 帮会（根据他们居住和攻击基地而命名）非法

进入了许多系统，甚至包括像 Los Alamos National Laboratory —— 一个核武器研究设施 —— 这样的绝密机构，他们终于被有关权力机关清查。

Legion of Doom 和 Chaos Computer Club 是两个开始在计算机和电子数据网络中探索弱点的先锋怪客组织。

Ian Murphy（又称 Captain Zap）非法进入了军事计算机，从公司商业订单数据库中窃取了信息，使用了被严格限制的政府电话交换台来打电话。由于他的这些入侵活动，美国国会在 1986 年投票通过了计算机欺诈和滥用法规（Computer Fraud and Abuse Act）。

根据这个法规，法庭才能够因为毕业生罗伯特 • 莫里斯（Robert Morris）把 Morris Worm 传播给 6000 多台连接到互联网上的计算机而给他定罪。按照这个法规裁决的另一例著名的案件是 Herbert Zinn。这名高中退学生非法闯入并滥用了属于 AT&T 和美国国防部的系统。

很多人担忧 Morris Worm 事件可能会重演，因此计算机紧急响应组（CERT）被创建来在网络安全问题上给计算机用户报警。

4.2.1.2.5 九十年代

ARPANet 被关闭。到该网络的交通都被转到互联网上。

Linus Torvalds 开发了 Linux 内核以用于 GNU 操作系统；对 Linux 的广泛开发和采用在很大程度上是用户和开发者通过互联网通信的结果。因为它源于 UNIX，Linux 在黑客和管理员中最为流行。他们发现 Linux 对于在运行专有（闭源）操作系统的早期服务器中建构另类安全措施很有帮助。

图形化万维网浏览器被创建，导致对公共互联网访问的需求迅速增加。

范德米尔 • 列文及其同伙闯入花旗银行的中央数据库，非法地将一千万美元巨额转入几个帐户。列文被 Interpol 逮捕，所有遗失款项都被追回。

凯文 • 米蒂尼克可能是所有怪客中最为先锋的一个。他闯入了几家大公司的系统，从著名人士的私人信息，两万余张信用卡帐号到软件的源码，他所窃取的信息包罗万象。他被逮捕并以电子贪污定罪，被判处了 5 年徒刑。

凯文 • 鲍尔森和一个不知名的同伙操纵了广播电台的电话系统来骗赢汽车

和奖金。他以计算机和电子贪污定罪，也被判处了 5 年徒刑。

非法闯入和电话诈骗的故事已渐渐成为传奇。一些未来的怪客在一年一度的 DefCon 会议中集会庆祝非法入侵并彼此交换见解。

一名 19 岁的以色列学生被逮捕并以在波斯湾冲突期间多次非法闯入美国政府的系统而定罪。军方人员将其称为是美国历史上对政府系统"最有组织和系统化的攻击"。

为了对在政府系统中日益增多的安全破坏情况采取相应措施，美国司法部长 Janet Reno 组建了国家机构设施保护中心。

英国通讯卫星被未知违法者劫获并绑票，英国政府最终夺回了卫星控制权。

4.2.1.3 当前的安全性

在 2000 年 2 月，互联网上几个流量最繁忙的站点遭到了一次分布型拒绝服务（DDoS）攻击。这次攻击使 yahoo.com、cnn.com、amazon.com、fbi.gov 和许多其它站点完全无法被正常用户使用，因为它使用大字节的 ICMP 分组传输（又称试通洪流、ping flood）把这些站点的路由器困住了几个小时。一群未知攻击者使用专门创建的、可广泛获取的程序来扫描防守薄弱的网络服务器；在这些服务器上安装叫做特洛伊木马（trojan）的客户程序；然后安排了一个攻击时间，让每个受感染的服务器满负荷地向受害站点发出分组，从而使受害站点变得不可用。

据统计：

- 在任意一天内，报告到卡内基－梅隆大学的 CERT 协调中心的主要安全破坏事件约有 225 起。
- 在 2003 年，报告到 CERT 的事件从 2001 年的 52,658 起和 2002 年的 82,094 起剧增到 137,529 起。
- 在过去三年中出现的三个最危险的互联网病毒对世界经济的影响估计约为 132 亿美元。

计算机安全已经渐渐成为信息工程预算中的一项必要的开支。那些要求数据完好性和高可用性的机构借助系统管理员、开发者、和工程师们的技术

力量来保证它们的系统、服务和信息的可靠性。恶意用户、进程、或协调攻击是对企事业的直接威胁。

然而，系统安全和网络安全是一项难题，它需要你对某个组织如何对待、使用、处理、以及传输信息有深入的了解。理解某个组织（以及组成它的所有人员）的运转方式对于实施正确的安全计划来说至关重要。

4.2.1.4 安全标准化

各行业的企业都依赖于如美国医疗协会（AMA）或电气和电子工程师学会（IEEE）这样的机构所设置的法则和规定。信息安全也不例外。许多安全顾问和厂商都认同一个叫做 CIA，或保密性、完好性、和可用性（Confidentiality, Integrity, and Availability）的标准安全模型。这个三层模型是用来评测保密信息所面临的危险以及建立安全策略的被普遍接受的安全标准的一个组成部分。以下详细描述了 CIA 模型：

保密性 —— 保密信息必须只能够被一组预先限定的人员存取。对这类信息的未经授权的传输和使用应该被严格限制。例如，信息保密性会确保顾客的个人和财务信息不被未经授权的人员获取以用于窃取身份或信用卡贪污之类的不良企图。

完好性 —— 信息不应该被能够导致它不完整或不正确的方式改变。未经授权的用户不应该具备修改或破坏保密信息的能力。

可用性 —— 信息应该能够被授权的用户在任何需要的时候都可以被存取。可用性是信息能够在规定的时间范围内、按照规定的频率而能够被获取的保证。这通常是按照百分比来衡量的，并且被网络服务器提供者和他们的企业客户使用的服务级别协议（SLA）正式达成协议。

4.2.2 安全控制

计算机安全经常被分成三大特性鲜明的主要类别，一般被称为"控制"：

- 物理控制
- 技术控制

- 管理控制

这三大类别定义了安全实现的主要目标。这些控制之中还有一些子类别，它们更进一步描述了控制以及如何实现这些控制。

4.2.2.1 物理控制

物理控制是一种在被明确规定的结构内实现安全性的措施。它用来防范或防止对保密资料未经授权的存取。物理控制的例子有：

- 闭路监控照相机
- 动作或热像报警系统
- 警卫人员
- 照片证件
- 上锁的和带有锁定插销的钢门
- 生物测定（包括指纹、声音、面孔、瞳孔、笔迹、以及其它用来识别个人的自动化方法）

4.2.2.2 技术控制

技术控制使用技术作为对整个物理结构内和网络中的机密数据进行控制的基础。技术控制的范围比较广，它包括的技术有：

- 加密
- 智能卡
- 网络验证
- 访问存取控制列表（ACL）
- 文件完好性审查软件

4.2.2.3 管理控制

管理控制定义了安全问题在人员方面的因素。它涉及了机构中所有级别的

人员，并使用类似以下的方法来决定哪些用户可以存取哪些资源：

- 培训和警惕性
- 灾难预备和恢复计划
- 人员招聘和分工策略
- 人员注册和记录

4.2.3 结论

了解了安全问题的起源、成因、以及其它相关因素后，就可以决定对 GTES10 进行恰当的配置。了解安全问题的因素和条件对于计划和实施正确的策略至关重要。掌握了相关信息后，这个过程就可以规范化，思路就会更开阔。

4.3 攻击者和漏洞

为了设计和实现一个良好的安全策略，我们首先要明确攻击者攻击和破坏系统的动机。在详细阐明这些问题前，我们首先定义相关的术语。

4.3.1 黑客简明历史

黑客（hacker）这个术语的现代意义起源于 1960 年的麻省理工学院（MIT）技术模型铁路俱乐部。"黑客"被用来称呼那些发现了聪明技巧或问题的绕行措施的俱乐部成员。

从那以后，"黑客"这个术语就被用来描述从计算机迷到具有天赋的编程员之类的人士。多数黑客的共同之处是他们对计算机系统和网络的自发的探索精神。开源软件开发者经常认为自己和他们的同事是黑客，并且把这个称谓当作一种尊称。

典型的黑客都遵守一种黑客道德（hacker ethic）。它要求黑客必须追求专业知识和技能，和社区分享这些知识和技能是每个黑客的职责。某些黑客会

从规避计算机系统的安全控制的学术挑战中获得乐趣，由于这个原因，新闻媒界经常使用"黑客"这个术语来描述那些蓄意地、带有犯罪意图的非法进入系统和网络的人。描述这类人的更恰当的用语应该是怪客（cracker）—— 被黑客在八十年代中期创造出来的术语，用来区分这两个社区。

4.3.1.1 灰度

寻找和利用系统和网络漏洞的人被区分成不同种类。这种类别是按照他们在进行安全漏洞调查时所"戴"的帽子颜色来区分的。帽子的颜色代表了他们的企图。

白帽黑客（white hat hacker）测试网络和系统的性能来判定它们能够承受入侵的强弱程度。通常，白帽黑客攻击他们自己的系统，或被聘请来攻击客户的系统以便进行安全审查。学术研究人员和专职安全顾问就属于白帽黑客。

黑帽黑客（black hat hacker）是怪客的同义词。通常来说，怪客并不注重于入侵系统的编程或学术方面。他们经常为了个人利益而依靠现成的攻击程序和著名的系统漏洞弱点来发现保密信息，或破坏目标系统或网络。

灰帽黑客（grey hat hacker）在多数情况下都具备白帽黑客的技术和意图，但是偶尔也使用这种知识来进行不太光明正大的行径。灰帽黑客可以被认为是偶尔会为个人企图而戴着黑帽的白帽黑客。

典型的灰帽黑客会遵循另一种黑客道德。他认为闯入系统是无可非议的，只要不进行盗窃行为或破坏保密信息就可以。不过，某些人可能会说，闯入系统本身就是不道德的。

不管入侵者的意图如何，了解怪客会试图利用的漏洞这一点都很重要。本章的剩余部分将会集中讨论这些问题。

4.3.2 对网络安全的威胁

在配置网络的以下方面时，某些不良习惯会增加系统被攻击的危险性。

4.3.2.1 不安全的体系

配置不良的网络是未经授权用户的主要入口。把基于信任的开放型本地网络向极不安全的互联网敞开就如同住在罪案重重的街区里却夜不闭户一样，在一段时间内可能会平安无事，但是最终总会有人要利用这个机会。

4.3.2.1.1 广播式网络

系统管理员经常忽略联网硬件在安全计划里的重要性。简单的硬件，如集线器和路由器，依赖广播或非转换的原理；这就是说，不管什么时候某个节点通过网络来传输数据，集线器或路由器都会广播这些数据分组，直到接收节点收到并处理这些数据为止。这种方法最容易被外界入侵者和本地未经授权的用户施行地址解析协议（arp）或媒体访问控制（MAC）的地址假冒攻击。

4.3.2.1.2 中央化的服务器

另一种潜在的联网危险是对中央化计算系统的使用。许多企事业中最常使用的节省开支措施是把所有的服务都集中于单个功能强大的机器上。中央化的服务器也给网络带来了单一失效点的问题。如果中央服务器被攻击了，这就会导致整个网络瘫痪，甚至造成数据被篡改或盗窃。在以上这些情况下，中央服务器就成为一个敞开的大门，允许任何人进入整个网络。

4.3.2.1.3 中央化的服务器

另一种潜在的联网危险是对中央化计算系统的使用。许多企事业中最常使用的节省开支措施是把所有的服务都集中于单个功能强大的机器上。中央化的服务器也给网络带来了单一失效点的问题。如果中央服务器被攻击了，这就会导致整个网络瘫痪，甚至造成数据被篡改或盗窃。在以上这些情况下，中央服务器就成为一个敞开的大门，允许任何人进入整个网络。

4.3.3 对服务器安全的威胁

服务器安全和网络安全同等重要，这是因为服务器中常常贮存着机构内部的大量重要信息。如果一个服务器泄密了，其中的所有内容都可以被怪客随心所欲地利用。以下各节讨论了一些主要问题。

4.3.3.1 未用的服务和打开的端口

GTES10 的完整安装包括 1000 个以上应用程序和库软件包。不过，多数服务器管理员并不打算安装发行版本中的每个软件包，而倾向于进行基本安装，再包括几个服务器程序。

系统管理员常常安装了操作系统却不关注那些被安装了的程序。这可能会导致问题，因为不需要的服务可能会被安装，并使用默认设置配置，而且可能还被默认启用。这就会导致不需要的服务，如 Telnet、DHCP、或 DNS 在服务器或工作站上运行，而管理员对此却一无所知。由此而带来的到该服务器的不必要的网络流量，甚至给怪客制造了一条潜在的路径。

4.3.3.2 未打补丁的服务

多数被包括在默认安装中的服务器程序是稳定的、被全面测试过的软件。在生产环境中被使用了多年后，这些软件的源码已经被全面精化，许多软件中存在的错误已被发现并修正。

然而，这些软件依然有潜在的 BUG。除此之外，由于新的软件在生产环境中的使用时间不长，或者因为它没有其它服务器软件那么流行，它可能没有被全面测试过。

开发者和系统管理员经常会在服务器程序中发现可被当作漏洞利用的程序错误，并在错误跟踪和安全相关的网站（如 Bugtraq 邮件列表：http://www.securityfocus.com）或计算机紧急响应组（CERT）的网站（http://www.cert.org）上公开这些信息。虽然这些机制是向社区发出安全漏洞警告的有效方法，但它却要依靠管理员来及时地给各自的系统打补丁。如果怪客也能够获得这些漏洞，他们就会使用这些信息来攻击未加补丁的

系统。优秀的系统管理需要时刻警惕、及时跟踪错误、并且进行正确的系统维护来保证安全的计算环境。

4.3.3.3 管理疏忽

忘记给系统打补丁是威胁服务器安全的最大因素。据系统管理网络和安全学院（System Administration Network and Security Institute，SANS）调查，计算机安全漏洞的主要原因是"指派未经培训的人员来维护安全，并且不提供使其能够胜任的培训和时间"。这不仅是指那些没有经验的管理员，也是指那些大意的管理员。

某些管理员忘记了给他们的服务器和工作站打补丁，而另一些则忘记了查看来自系统内核或网络的日志消息。另一个常见错误是不改变服务的默认口令或密码。例如，某些数据库有默认的管理口令，因为数据库开发者假定系统管理员在安装后会立即改变这些口令。如果某个数据库管理员忘记了改变口令，甚至一个毫无经验的怪客也能够使用众所周知的默认口令来获得到数据库的管理特权。

4.3.3.4 具有不安全因素的服务

如果所选的网络服务有固有的不安全因素，即便是警惕性最高的组织也可能成为受害者。例如，许多服务是在用于可信任网络的假定条件下被开发的；然而，一旦这些服务可通过互联网被使用，这个假定条件就不适用了。互联网本身就带有固有的不可信任性。

还有一类不安全网络服务是那些需要用户名和口令来验证的服务。Telnet 和 FTP 就属于这类服务。如果分组嗅探软件正在监视远程用户和这类服务器间的通信，口令就能够被轻易地窃取。

以上提及的服务还会轻易地遭到安全行业称之为"中间人"（man-in-the-middle）的攻击。在这类攻击中，怪客会设计让网络上的一个已攻破的名称服务器指向自己的机器而不是实际的目标服务器来重新导向网络交通。一旦某人打开了一个到该服务器的远程会话，怪客的机器就会充当一个隐型导管，在毫不知情的远程服务和用户间截取信息，怪客可以

用这种方法来收集管理性口令和原始数据。

另一类不安全服务是网络文件系统和信息服务，如 NFS 或 NIS。它们仅仅是为 LAN 而开发的，但不幸的是，后来又被扩展来包括 WAN（以方便于远程用户）。按照默认设置，NFS 没有配置任何验证或安全机制来防止怪客挂载 NFS 共享存取其中的数据。同样的，NIS 也有网络上的每个计算机都的重要信息，包括口令和文件权限。它们都存在于一个纯文本的 ACSII 或 DBM（由 ASCII 推导出的）数据库中。能够进入这个数据库的怪客就能够获得网络上的每个用户帐号，包括管理员的帐号。

按照默认设置，GTES10 的发行版本关闭此类服务。如果管理员不得不使用这些服务，谨慎配置就至关重要。

4.3.4 对工作站和家用电脑安全性的威胁

工作站和家用电脑对攻击者的吸引力可能不会像网络或服务器那么大，但是由于其上经常包含保密信息，如信用卡信息，也被怪客看中。工作站还能够被怪客在协调攻击中被用作"从属"机器，而其主人对此却一无所知。由于这些原因，了解工作站的弱点能够帮助用户避免重新安装操作系统的麻烦。

4.3.4.1 不良口令

不良口令是攻击者获得对系统访问权的最简单的方法之一。

4.3.4.2 有漏洞的客户应用程序

管理员可能会配置一个完全安全的、全面打过补丁的服务器，但这并不意味着远程用户在进入它时就是安全的。例如，如果服务器提供经由公共网络的 Telnet 或 FTP 服务，攻击者可能会在纯文本用户名和口令在网络中经过时劫获它们，然后使用这个帐号信息来进入远程用户的工作站。

甚至在使用安全协议如 SSH 的时候，如果远程用户没有更新他们的客户程序，他们也可能遭受某些攻击。例如，使用 SSH 第一版本的用户就有可能

遭受来自恶意的 SSH 服务器的 X 转发攻击。一旦连接到了服务器上，攻击者就能够不动声色地截取客户通过网络进行的击键和鼠标点击。这个问题在 SSH 协议的第二版本中被修正了，但是它却要依赖于用户自身的自觉性，看他是否关注哪些应用程序有哪些弱点，并在必要时更新这些程序。

4.4 GTES10 安全更新

该部分为管理员提供了保护 GTES10 安全更新的方法。

当发现了安全漏洞后，你必须更新相关的软件以便把潜在的安全威胁限制在一定范围内。如果该软件是目前 GTES10 发行版本的一部分，Turbolinux, Inc. 会保证尽快地发行修正漏洞的更新软件包。在某个安全漏洞被宣布的同时通常会附带补丁（或修正问题的源码）。然后，该补丁就会被应用到 GTES10 软件包中，当它被 Turbolinux 的质检组测试后就会作为勘误更新而被发行。

4.4.1 更新软件包

在更新系统上的软件包时，从可信任源下载它们至关重要。某个攻击者可以轻易地使用修正问题的同一版本号来重新对软件打包，却在其中隐藏另一种安全漏洞，然后在互联网上发行。因此，从可信任源（如 Turbolinux, Inc.）下载 RPM，并检查软件包的签名来校验它的完好性这一点至关重要。

4.4.1.1 校验被签名的软件包

所有的 GTES10 软件包都使用 Turbolinux, Inc. GPG 钥匙签名。GPG 代表 GNU Privacy Guard 或 GnuPG。它用来确保发行文件的真实性。例如，拓林思拥有的私钥（或密钥）会锁住软件包，而公钥可以打开并校验软件包。如果在 RPM 校验过程中，拓林思发行的公钥和密钥不匹配，该软件包就可能被篡改了，因此不可信任。

GTES10 中的 RPM 工具会在安装软件包前自动校验它的 GPG 签名。如果

你没有安装 Turbolinux, Inc. GPG 公钥，请从一个安全、静态的位置（如 GTES10 安装光盘）上安装它。

假定光盘被挂载在/mnt/cdrom，使用以下命令来把它导入到你的钥匙圈上（keyring，系统上可信任钥匙的数据库）：

```
rpm --import /mnt/cdrom/RPM-GPG-KEY
```

要显示所有已安装的用于 RPM 校验的公钥列表，执行以下命令：

```
rpm -qa gpg-pubkey*
```

Turbolinux 公钥的输出会包括：

```
gpg-pubkey-db42a60e-37ea5438
```

要显示特定公钥的细节，使用 rpm -qi 命令，和前一命令的输出。在这个例子中是：

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

在安装 RPM 文件前校验它的签名这一个步骤至关重要，只有这样才能确保这些文件没有从 Turbolinux, Inc. 软件包的发行版本中被篡改。要立刻校验所有已下载的软件包，使用以下命令：

```
rpm -K /tmp/updates/*.rpm
```

对于每个软件包，如果 GPG 钥匙校验成功，该命令会返回：gpg OK。否则，确认你使用的是正确的拓林思公钥，并校验其内容。没有通过 GPG 校验的软件包不应该被安装，因为它们可能已经被第三方篡改了。

校验了 GPG 公钥，并下载了所有和勘误报告有关的软件包后，在 shell 提示下以根用户身份安装它们。

4.4.1.2 安装被签名的软件包

对多数软件包（除了内核软件包外）来说，你可以使用以下命令来安全地安装：

```
rpm -Uvh /tmp/updates/*.rpm
```

安装内核软件包应使用以下命令：

```
rpm -ivh /tmp/updates/<kernel-package>
```

把前一个例子中的 <kernel-package> 改成内核 RPM 的名称。

一旦系统使用新内核被安全引导后，你可以使用以下命令来删除老内核：

```
rpm -e <old-kernel-package>
```

把前一个例子中的 <old-kernel-package> 改成老内核 RPM 的名称。

4.4.1.3 应用改变

通过拓林思勘误网站下载并安装了安全勘误后，停用旧有软件而使用新软件这一点很重要。以下的列表详细列举了软件的一般类别，并为更新软件包后使用被更新的版本提供了说明。

- 应用程序

用户空间的应用程序是能够被系统用户执行的任何程序。通常，这类程序只有在某用户、脚本、或自动化任务工具启动它们时才被使用，而且并不持续运行很久。

当这类用户空间的应用程序被更新后，停运系统上该程序的所有实例，然后再重新启动它来使用更新的版本。

- 内核

内核是 GTES10 操作系统的核心软件组成部分。它管理内存、处理器和外设的使用，还进行所有的任务调度。由于这种核心角色，必须重启计算机才能重新启动内核。因此，在系统被重新引导前，更新的内核版本就无法被使用。

- 共享库

共享库是编码单元的集合，例如 glibc 被许多应用程序和服务所使用。使用共享库的应用程序通常在初始化的时候载入共享编码，因此使用已更新的共享库的应用程序必须重新启动。

要判定哪些链接到某个共享库的应用程序正在运行，使用 lsof 命令，如以下所示：

```
lsof /usr/lib/libwrap.so*
```

该命令返回一个使用 TCP 会绕程序来进行主机访问控制的所有正在运行的程序的列表。因此，如果 tcp_wrappers 软件包被更新了，所有列举了的程序都必须被停运并被重新启动。

- SysV 服务

SysV 服务是在引导过程中启动的持续性服务器程序。SysV 服务的例子包括：sshd、vsftpd、和 xinetd。

因为只要机器被启动了，这些程序就通常持久性地滞留在内存中，所以每个更新了的 SysV 服务在软件包升级后必须重新启动。你可以使用服务配置工具完成，或登录到根用户的 shell，然后使用 /sbin/service 命令，如以下所示：

```
/sbin/service <service-name> restart
```

在前面的例子中，把 <service-name> 改成服务的名称，如 sshd。

- xinetd 服务

由 xinetd 这个超级服务控制的服务只有在有活跃连接时才运行。由 xinetd 控制的服务包括：Telnet、IMAP、和 POP3。

因为这些服务的新实例是在每次 xinetd 收到新请求时被启动的，升级后的连接就会由已更新的软件来处理。然而，如果由 xinetd 控制的服务在被升级时还存在着一些活跃连接的话，这些连接就会由软件的老版本处理。

要停止某个 xinetd 控制的服务的早期实例，升级和该服务相应的软件包，然后停止所有当前正在运行的进程。使用 ps 命令来判定进程是否在运行，再使用 kill 或 killall 命令来停运该服务的所有当前实例。

例如：如果 imap 软件包的安全勘误被发行了，升级这些软件包，然后以根用户身份在 shell 提示下键入以下命令：

```
ps -aux | grep imap
```

该命令返回所有活跃的 IMAP 会话。使用以下命令可以终止单个会话：

```
kill -9 <PID>
```

在前面的例子中，把 <PID> 替换为 IMAP 会话的进程号码（在 ps 命令输出的第二列）。

要杀死所有活跃的 IMAP 会话，使用以下命令：

```
killall imapd
```

4.5 GTES10 工作站安全

保护 Linux 环境的安全应从工作站开始。无论是锁定个人机器还是保护企业系统，可靠的安全策略都应从个体计算机开始。一个计算机网络的安全取决于最弱的环节。

4.5.1 评估工作站的安全性

在评估 GTES10 工作站的安全性时，请考虑以下因素：

- BIOS 和引导装载程序的安全性 —— 未经授权的用户是否能够亲手使用机器，并不必使用口令而引导单用户或救援模式？
- 口令安全 —— 机器上的用户帐号的口令有多安全？
- 管理控制 —— 谁在系统上有帐号？他们有多大的管理权？
- 可用的网络服务 —— 哪些服务在监听网络上的请求？它们应不应该运行？
- 个人防火墙 —— 哪类防火墙是必要的？
- 经安全强化的通信工具 —— 哪些工具应该被用来在工作站直接通信？哪些应该避免使用？

4.5.2 BIOS 和引导装载程序的安全性

使用口令保护 BIOS 和引导装载程序可以防止那些可以在物理上接近系统的未经授权的用户使用移动介质来引导或通过单用户模式来获得根权限。

但是防御这类攻击的安全措施既依赖于工作站上信息的保密程度，也依赖于机器的地点。

例如，如果机器在展销会上被使用，并且不包含任何保密信息，可能防御这类攻击就不那么重要。然而，如果在同一个展销会上，某个雇员的便携电脑无人看管，但是其中含有公司网络的未加密的 SSH 密钥，它就可能会导致影响整个公司的重大安全问题。

从另一方面考虑，如果工作站位于只有被授权或被信任的人员才能进入的地方，那么保护 BIOS 或引导装载程序的安全性可能就根本不必要。

4.5.2.1 BIOS 口令

以下是使用口令来保护计算机 BIOS 的两个主要原因：

- 防止对 BIOS 设置的改变 —— 如果入侵者可以进入 BIOS，他们就可以把它设置为从软盘或光盘引导。这就使他们能够进入救援模式或单用户模式，从而允许他们在系统上放置恶意程序或复制保密数据。

- 防止系统被引导 —— 某些 BIOS 允许你使用口令来保护引导进程。当激活时，攻击者在 BIOS 启动引导装载程序前就不得不输入口令。

因为设置 BIOS 口令的方法因计算机厂商而各有不同，请参考你的计算机手册来获得特有说明。

如果你忘记了 BIOS 口令，可以通过主板上的跳线或断开 CMOS 电池的连接来重设。由于这个原因，在可能的时候最好能锁住电脑。

4.5.2.2 引导装载程序口令

以下是使用口令来保护 Linux 引导装载程序的主要原因：

- 防止进入单用户模式 —— 如果攻击者能够引导进入单用户模式，他就可以在不被要求输入根口令的情况下成为根用户。

- 防止进入 GRUB 控制台 —— 如果机器使用 GRUB 作为引导装载程序，攻击者可以使用 GRUB 编辑界面来改变它的配置或使用 cat 命令来收集信息。

- 防止进入非安全的操作系统 —— 如果它是双引导系统，攻击者可以在引导时选择操作系统，例如 DOS，它会忽略存取控制和文件权限。

GRUB 可以通过在它的配置文件中添加一个口令（password）指令来解决上述的前两个问题。要这么做，首先决定要使用什么口令，然后打开 shell 提示，登录为根用户，键入：

```
/sbin/grub-md5-crypt
```

在提示时，键入 GRUB 口令，然后按。这会返回一个口令的 MD5 散列。

下一步，编辑 GRUB 配置文件 /boot/grub/grub.conf。打开文件，在主体的 timeout 行下添加以下行：

```
password --md5 <password-hash>
```

把 <password-hash> 替换成 /sbin/grub-md5-crypt 返回的值：

下次系统引导时，如果你不首先按 p 和 GRUB 口令，GRUB 菜单就不会允许你进入编辑器或命令界面。

然而，这个办法并不能防止攻击者在双引导环境中引导不安全的操作系统。要解决这个问题，你必须编辑 /boot/grub/grub.conf 文件中的另一个部分。

寻找不安全操作系统的 title 行，然后紧跟在下面添加一行 lock。

对于 DOS 系统，该实例应该和以下的启动方式相似：

```
title DOS

lock
```

要为某个特定内核或操作系统创建不同的口令，在那个实例中添加一个 lock 行，再紧跟一个 password 行。

每个使用特定口令来保护的实例开头都应该和以下相似：

```
title DOS

lock

password --md5 <password-hash>
```

4.5.3 口令安全

口令是 GTES10 用来校验用户身份的首要方法。因此保护口令的安全性对于用户、工作站以及整个网络来说都是极端重要的。

为了安全，安装程序配置系统使用 MD5（Message-Digest Algorithm）和屏蔽口令。

如果安装时没有选择使用 MD5 口令，较老的数据加密标准（Data Encryption Standard，DES）格式就会被使用。该格式把口令限定为八个字母数字字符（不允许标点和其它特殊字符），并且提供了普通的 56 位级别的加密。

如果屏蔽口令在安装中被取消选择，所有的口令就会作为单向散列被保存在全局可读的/etc/passwd 文件中，这使系统非常容易受到离线口令破译攻击。如果入侵者可以作为普通用户进入机器，他就能够把/etc/passwd 文件复制到他自己的机器上，然后运行多种口令破译程序。如果文件中有不安全的口令，那么口令怪客找到它就只是个时间问题。

屏蔽口令通过把口令散列保存在/etc/shadow 文件中而使系统免遭此类攻击，因为该文件只能被根用户读取。

这会迫使潜在的攻击者通过登录到机器上的服务如 SSH 或 FTP 来试图进行远程口令破译。这类强力破译非常缓慢，并且会留下很明显的踪迹，因为系统文件中会记录上百次失败了的登录企图。当然，如果怪客在夜半三更时试图破译系统上的薄弱口令，他们可能会在凌晨前进入系统，从而编辑日志文件来掩盖其踪迹。

除了格式和贮存方式，口令内容是另一个值得考虑的因素。用户保护其帐号免受口令破译攻击的最重要措施是创建一个强健的口令。

4.5.3.1 创建强健的口令

在创建安全口令的时候，最好能遵循以下准则：

应该防止的做法：

- 不要只使用单词或数字 —— 决不要在口令中只使用单词或数字。

某些不安全口令包括：

8675309

juan

hackme

- 不要使用现成词汇 —— 像名称、词典中的词汇、甚至电视剧或小说中的用语，即使在两端使用数字，都应该避免使用。

某些不安全口令包括：

john1

DS-9

mentat123

- 不要使用外语中的词汇 —— 口令破译程序经常使用多种语言的词典来检查其词汇列表。依赖外语来达到保护口令的目的通常不起作用。

某些不安全口令包括：

cheguevara

bienvenido1

1dumbKopf

- 不要使用黑客术语 —— 如果你以为在口令中使用黑客术语 —— 又称 l337 (LEET) —— 就会与众不同，请再三思。许多词汇列表都包含了 LEET 式术语。

某些不安全口令包括：

1337

H4X0R

- 不要使用个人信息 —— 千万不要使用个人信息。如果攻击者知道你的身份，推导出你所用口令的任务就会变得非常容易。以下是你在创建口令时应该避免使用的信息类型。

某些不安全口令包括：

你的名字

宠物的名字

家庭成员的名字

生日

你的电话号码或邮政编码

- 不要倒转现存词汇 —— 优秀的口令破译者总是倒转常用词汇，因此倒转薄弱口令并不会使它更安全。

某些不安全口令包括：

nauj

9-DS

H4X0R

- 不要笔录你的口令 —— 决不要把口令写在纸上。把它牢记在心才更为安全。

- 不要在所有机器上都使用同样的口令 —— 在每个机器上使用不同的口令是及其重要的。这样，如果一个系统泄密了，所有其它系统都不会立即受到威胁。

推荐的做法：

- 口令长度至少为八个字符 —— 口令越长越好。若使用 MD5 口令，它应该至少有 15 个字符。若使用 DES 口令，使用最长长度（8 个字符）。

- 混和大小写字母 —— GTES10 区分大小写，因此混和大小写会增加口令的强健程度。

- 混和字母和数字 —— 在口令中添加数字，特别是在中间添加（不只在开头和结尾处）能够加强口令的强健性。

- 包括字母和数字以外的字符 —— &、$、和 > 之类的特殊字符可以极大地增强口令的强健性（若使用 DES 口令则不能使用此类字符）。

- 挑选一个你可以记住的口令 —— 如果你记不住你的口令，那么它再好也没有用；使用简写或其它记忆方法来帮助你记忆口令。

以下是一种可以用来生成可记忆的安全口令的步骤：

- 想出一个可记忆的短语，如：

"over the river and through the woods, to grandmother's house we go."

- 然后只引用第一个字母而把它变成简写（包括标点）。

otrattw,tghwg.

- 把简写中的字母替换成数字和符号来增加其复杂性。例如，用 7 来替换 t，用 @ 来替换 a：

o7r@77w,7ghwg.

- 至少把一个字母变成大写来增加其复杂性，如 H。

o7r@77w,7gHwg.

- 最后，不要在任何系统上使用以上的口令范例。

创建安全口令的重要性不言而喻，正确地管理它们也极为重要，特别是对于大机构的系统管理员来说。下节讨论了如何在机构中有效地创建和管理用户口令。

4.5.3.2 在机构内创建用户口令

若机构内的用户数量很大，系统管理员可以使用两种基本方法来强制使用好口令。他们可以为用户创建口令，或者让用户自行创建口令，但是校验该口令是否可被接受。

为用户创建口令会保证这些口令是强健的，但是随着机构的扩大，这项任务也会变得越来越繁琐。它还会导致用户把口令写下来。

由于这些原因，系统管理员更喜欢让用户自行创建口令，然后再积极地校验这些口令是否可被接受，在某些情况下，通过口令老化来强制用户定期改变口令。

4.5.3.2.1 强制使用强健口令

要保护网络免受入侵攻击，系统管理员应该校验机构内使用的口令是否强健。当用户被要求创建或改变口令时，他们可以使用命令行程序 passwd 来进行。该程序能够识别可插入验证管理器（Pluggable Authentication Manager，PAM），因此它会根据 pam_cracklib.so 这个 PAM 模块来检查口令是否容易被破译或是否太短。由于 PAM 是可被定制的，你可以进一步添加口令完好性检查器，如 pam_passwdqc（可在 http://www.openwall.com/passwdqc/ 获得），或编写一个新模块。要获取可用 PAM 模块的列表，请查看 http://www.kernel.org/pub/Linux/libs/pam/modules.html。不过，应该注意的是，在创建口令时进行的检查不能像运行口令破译程序那样有效地发现不良口令。

以下是一些较流行的口令破译程序的简单列表：

- John The Ripper —— 一个快速而灵活的破译程序。它允许使用多个词汇列表，并且具有强力破译的能力。在 http://www.openwall.com/john/ 中可以获得。

- Crack —— 也许是最著名的口令破译软件。Crack 虽然没有 John The Ripper 那么容易使用，但运行速度很快。可以在 http://www.crypticide.org/users/alecm/ 上找到。

- Slurpie —— Slurpie 与 John The Ripper 和 Crack 相似，但它被设计可在多机上同时运行，创建了一种分布型口令破译攻击。在 http://www.ussrback.com/distributed.htm 上可以找到它以及其它分布型攻击的安全评估工具。

4.5.3.2.2 口令老化

口令老化是系统管理员用来防止机构内不良口令的另一种技术。口令老化意味着过了一段预先设定的时间后（通常是 90 天），用户会被提示创建一个新口令。它所根据的理论是，如果用户被强制定期改变口令，某个破译的口令对入侵者来说就只有有限的利用机会。不过，口令老化的不利性是，用户很可能会把他们的口令写下来。

GTES10 中用来指定口令老化的两个主要程序是：chage 命令和图形化的用户管理器（system-config-users）程序。

chage 命令的-M 选项指定口令的最长有效期。例如，要把用户的口令设置为 90 天后过期，键入以下命令：

```
chage -M 90 <username>
```

在上面的命令中，把 <username> 替换成用户名。如果不想让口令过期，传统方法是在 -M 选项后使用 99999（这相当于 273 年）。

图形化的用户管理器程序也可以被用来创建口令老化策略。在 shell 提示下（如 XTerm 或 GNOME 终端）键入 system-config-users 命令。点击“用户”活页标签，从用户列表中选择用户，然后点击按钮菜单上的“属性”（或从拉下菜单中选择“文件 —> 属性”。

然后点击“口令信息”活页标签，输入口令过期的天数，如图 4-1 所示。

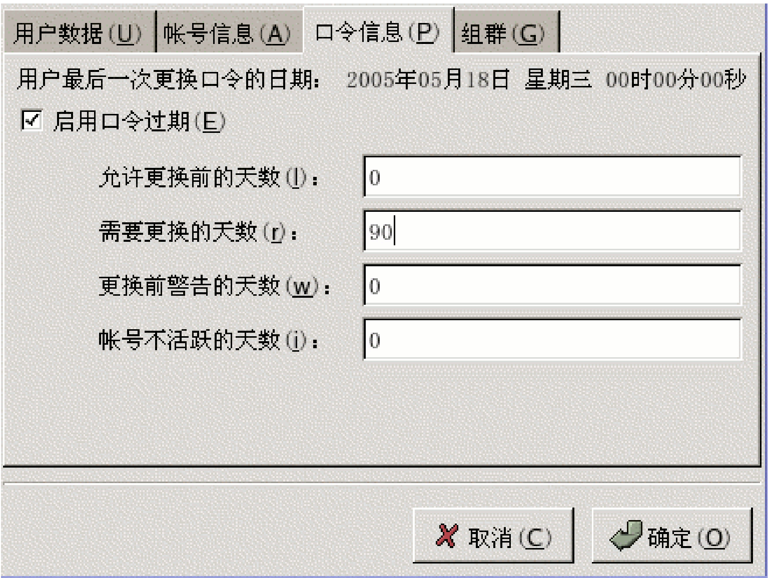


图 4-1 “口令信息”面板

4.5.4 管理控制

在家用计算机中，用户必须以根身份或通过 setuid 程序（如 sudo 或 su）而获得有效根特权来执行某些任务。setuid 是一种使用程序所有者的用户 ID（UID）而不是运行该程序的用户 ID 的程序。当使用长格式列举时，这类程序的所有者部分有一个小写的 s，如下所示：

```
-rwsr-xr-x    1 root     root       47324 May   1 08:09 /bin/su
```

然而，对于一个机构的系统管理员来说，他们必须决定机构内的用户对机器到底能拥有多少管理权限。通过 pam_console.so 这个 PAM 模块，某些通常保留给根用户的活动，如重新引导和挂载可移介质，第一个登录到实际控制台的用户也会被允许进行操作。然而，其它重要的系统管理任务，如改变网络设置、配置新鼠标、或挂载网络设备，没有管理权限就无法进行。因此，系统管理员必须决定网络上的用户可以拥有多少管理权限。

4.5.4.1 允许根权限

如果机构内的用户是可信任的，给用户拥有根权限意味着一些类似添加设备或配置网络接口的小事情可以被用户自己处理，因此系统管理员就有时间处理网络安全和其它重要的任务。

但是从另一方面来说，给个人用户以根权限会导致以下问题：

- 机器的错误配置 —— 具备根权限的用户可能会错误配置他们的机器，从而需要协助；或者更糟的是打开安全漏洞而不自知。
- 运行不安全服务 —— 具备根权限的用户可能会在他们的机器上运行不安全的服务器，如 FTP 或 Telnet，从而在用户名和口令被明文传输时给它们带来潜在危机。
- 作为根用户运行电子邮件附件 —— 影响 Linux 的病毒虽然很罕见，但是并不是没有。不过，它们只有在以根用户身份运行的时候才会给系统造成威胁。

4.5.4.2 禁止根存取权限

如果管理员因为这些原因或其它原因对于允许用户登录为根用户认为不适合，就应该把根口令保密，并且通过使用口令保护引导装载程序来禁止进入运行级别 1 或单用户模式。

表 4-1 显示了管理员可以进一步保证根登录被禁止的方法：

方法	描述	影响	不影响
改变根 shell。	编辑 /etc/passwd 文件，然后把 shell 从 /bin/bash 改成 /sbin/nologin。	阻止进入根 shell 并记录所有进入企图。 以下程序会被阻止进入根帐号： login gdm kdm xdm su ssh scp sftp	不需要 shell 的程序，如 FTP 客户、邮件客户以及许多 setuid 程序。 以下程序不会被阻止进入根帐号： sudo FTP 客户 电子邮件客户。
禁止通过任何控制台设备（tty）来获得根权限。	一个空的 /etc/securetty 文件会防止任何连接在这个计算机上的设备以根用户登录。	防止通过控制台或网络来进入根帐号。 以下程序被禁止用来进入根帐号： login gdm kdm	不以根用户身份登录，却通过 setuid 或其它机制来执行管理性任务。 以下程序不会被禁止进入根帐： su

		xdm 其它打开 tty 的网络服务。	sudo ssh sftp
禁用根用户的 SSH 登录。	编辑 /etc/ssh/sshd_config 文件，把 PermitRootLogin 参数设置为 no。	防止通过 OpenSSH 工具套件来获得根权限。 以下程序会禁止进入根帐号： ssh scp sftp	这只会阻止根帐号对 OpenSSH 工具套件的使用。
使用 PAM 来限制根用户对服务的存取权限。	编辑 /etc/pam.d/ 目录中的表示目标服务的文件。为了验证的目的 pam_listfile.so 是需要的。	防止到识别 PAM 的网络服务的根使用权限。 以下服务不能进入根帐号： FTP 客户 电子邮件客户 login gdm kdm xdm ssh scp sftp 任何识别 PAM 的服务	不识别 PAM 的程序

表 4-1. 禁用根帐号的方法

4.5.4.2.1 禁用根 Shell

要防止用户直接登录为根用户，系统管理员可以在/etc/passwd 文件中把根帐号的 shell 设置为 /sbin/nologin。这会阻止需要 shell 的命令，如 su 和 ssh 等直接进入根帐号。

4.5.4.2.2 禁用根登录

要进一步限制对根帐号的使用权限，管理员可以通过编辑/etc/securetty 文件来禁用控制台的根登录。该文件列举了所有根用户被允许登录的设备。如果该文件不存在，根用户就能通过系统上的各类通信设备，不管是控制台还是原始网络接口登录。这种情况很危险，因为用户可以以根用户身份使用 Telnet 来登录，在网络中明文传送根口令。按照默认设置，GTES10 的 /etc/securetty 文件只允许根用户在和机器物理相连的控制台上登录。要阻止根用户登录，键入以下命令来清除该文件的内容:

```
echo > /etc/securetty
```

4.5.4.2.3 禁用根用户的 SSH 登录

要防止根用户通过 SSH 协议登录，编辑 SSH 守护进程的配置文件（/etc/ssh/sshd_config）。把以下一行：

```
# PermitRootLogin yes
```

改成：

```
PermitRootLogin no
```

4.5.4.2.4 使用 PAM 禁用根权限

PAM 通过/lib/security/pam_listfile.so 模块在拒绝特定帐号方面提供了极大的灵活性。这使管理员能够在禁止登录的用户列表上应用该模块。以下

的例子显示了该模块在 /etc/pam.d/vsftpd PAM 配置文件中的 vsftpd FTP 服务器上是如何被使用的：

```
auth      required      /lib/security/pam_listfile.so      item=user \
sense=deny file=/etc/vsftpd.ftpusers onerr=succeed
```

这告诉 PAM 参考 /etc/vsftpd.ftpusers 文件，并拒绝其中列举的用户使用该服务。管理员可以随意改变这个文件的名称，并为每个服务保存单独的列表，或使用一个单一列表来拒绝到多个服务的使用权限。

如果管理员要拒绝到多个服务的使用权限，可以在 PAM 配置服务（如 /etc/pam.d/pop 和用于邮件服务的/etc/pam.d/imap、或用于 SSH 客户的 /etc/pam.d/ssh）中添加相似的一行。

4.5.4.3 限制根存取权限

另外，管理员可能只想通过 setuid 程序如 su 或 sudo 等来允许对其的使用。

4.5.4.3.1 su 命令

键入 su 命令后，用户会被提示输入根口令，经验证后，他就会得到一个根 shell 提示。

通过 su 命令登录后，用户成为根用户，并且对系统有绝对的管理权。此外，一旦用户成为根用户，他还可以使用 su 命令来变成系统上的另一个用户而不必输入口令。

因为该程序非常强大，机构内的管理员可能想限制能够使用这个命令的人员。

最简单的方法是把用户添加到一个叫做 wheel 的特殊管理组群。要这么做，以根用户身份键入以下命令：

```
usermod -G wheel <username>
```

在前面的命令中，把 <username> 替换成被添加到 wheel 组群中的用户

名。

使用用户管理器可以同样达到这个目的。在 shell 提示下键入 system-config-users 命令。选择“用户”活页标签，从用户列表中选择该用户，然后点击按钮菜单上的“属性”（或从拉下菜单中选择“文件—>属性”）。

然后选择“组群”活页标签，点击 wheel 组群，如图 4-2 所示。

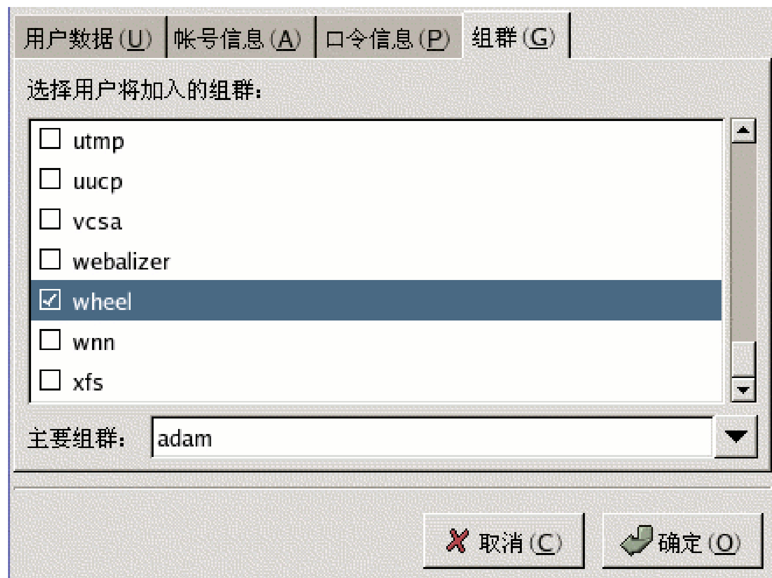


图 4-2 “组群”面板

下一步，在文本编辑器中打开 su（/etc/pam.d/su）的 PAM 配置文件，删除以下行的注释符号 ：

```
auth    required /lib/security/$ISA/pam_wheel.so use_uid
```

这样，只有管理性组群 wheel 才能使用该程序。

4.5.4.3.2 sudo 命令

sudo 命令提供了另一种授予用户管理权限的方法。当可信任的用户在管理命令前加一个 sudo 命令，这个用户就会被提示输入他自己的口令。验证

后，假定这个命令被准许执行，它就会以根用户身份执行。

sudo 命令的基本格式如下：

```
sudo <command>
```

在上面的例子中，<command> 应该被替换为通常保留给根用户使用的命令，如 mount。

sudo 命令提供了高度的灵活性。例如，只有列举在/etc/sudoers 配置文件中的用户被允许使用 sudo 命令，并且命令是在用户的而不是根的 shell 中被执行。这意味着根 shell 可以被完全禁用。

sudo 命令还提供了完整的审核渠道。每次成功的验证都被记录在/var/log/messages 文件中，所使用的命令以及使用者的用户名被记录在/var/log/secure 文件中。

sudo 命令的另一个优越性是，管理员可以根据需要给不同的用户以不同的命令使用权限。

可以使用 visudo 命令编辑 sudo 配置文件/etc/sudoers。

要给某人以完全的管理权限，键入 visudo，然后在用户特权规定部分添加和以下相似的一行：

```
juan ALL=(ALL) ALL
```

这个例子表明，用户 juan 可以在任何主机上使用 sudo 来执行任何命令。

以下的例子显示了 sudo 配置方面的可伸缩性：

```
%users    localhost=/sbin/shutdown -h now
```

这个例子表明，只要是从控制台使用，任何用户都可以使用/sbin/shutdown -h now 命令。

4.5.5 可用网络服务

对于系统管理员来说，控制用户对管理权限的使用是一个重要的问题；对于安装和操作 Linux 系统的人员而言，决定和控制哪些网络服务应该处于活跃状态就更为重要。

许多 GTES10 中的服务都像网络服务器一样。如果机器上运行某个网络服务，那么这个叫做守护进程（daemon）的服务器程序就在一个或多个网络端口上监听连接。每一个此类服务器都都是潜在的攻击渠道。

4.5.5.1 服务可能受到的威胁

网络服务可以给 Linux 系统带来许多威胁。以下列举了一些主要威胁：

• 拒绝服务攻击（DoS） —— 拒绝服务攻击通过向服务器发送大量服务请求使系统由于试图记录和答复每个请求而陷于停顿，从而无法响应正常的服务请求。

• 脚本漏洞攻击 —— 如果服务器使用脚本来执行服务器端的操作（http 服务器通常如此），怪客可以对不正确编写的脚本发起攻击。这些脚本漏洞能够导致缓冲溢出或允许攻击者改变系统上的文件。

• 缓冲溢出攻击 —— 连接到端口 0 到 1023 的服务必须以管理用户的身份运行。如果应用程序中有一个可利用的缓冲溢出漏洞，攻击者就能够在用户运行守护进程的时候获得对系统的控制权。由于可被利用的缓冲溢出的存在，怪客可以使用自动化的工具来识别有漏洞的系统，一旦他们获得进入权，他们可以使用自动化的 rootkits 来保持对系统的使用权。

要把受到网络攻击的暴露程度限制在一定范围内，你应该关闭所有不使用的服务。

4.5.5.2 识别和配置服务

为增强安全性，多数随 GTES10 一起安装的网络服务都被默认关闭。以下例外：

• cupsd —— GTES10 的默认打印服务器。

• lpd —— 另一个打印服务器。

• xinetd —— 控制连接到 vsftpd、telnet 之类的从属服务器的超级服务器。

• sendmail —— Sendmail 邮件传输代理被默认启用，但是它只监听

localhost 上的连接。

- sshd —— OpenSSH 服务器，是 Telnet 的安全替代品。

在决定是否让这些服务继续运行时，需小心谨慎。例如，如果没有打印机，就不必运行 cupsd。portmap 端口也同理，如果不挂载 NFSv3 文件卷或使用 NIS（ypbind 服务），那 portmap 就应该被禁用。

GTES10 中包括了三个用来开关服务的程序。它们是：服务配置工具（system-config-services）、ntsysv 和 chkconfig。

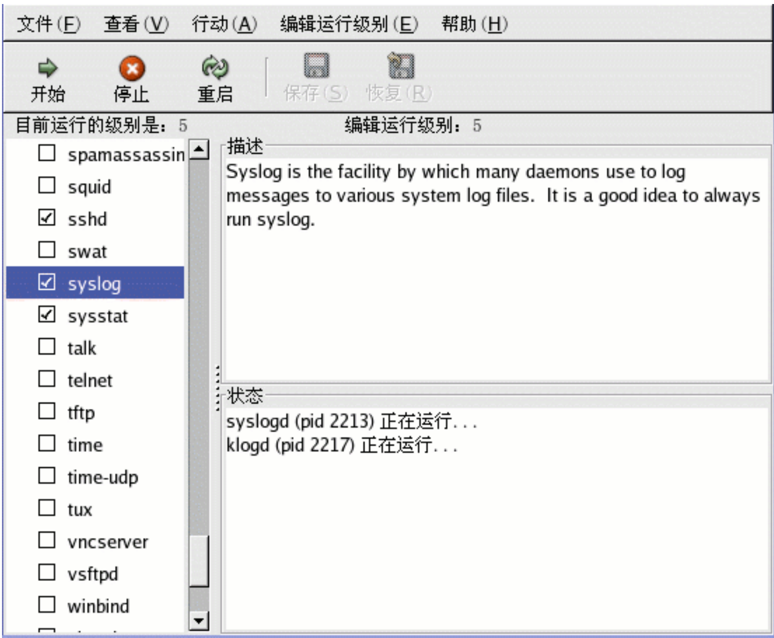


图 4-3 服务配置工具

如果对某服务的目的不清楚，服务配置工具中有描述字段可以参考，如图 4-3 所示。

但是仅仅查看哪些网络服务在引导时被启用是不够的。系统管理员还应该检查哪些端口被打开或正在监听。

4.5.5.3 不安全服务

任何网络服务都有潜在的不安全因素。关闭不使用的服务非常重要。服务漏洞会被例行检查、提出和修补，因此，更新与网络服务有关的软件包格外重要。

某些网络协议具有固有的不安全因素。这些协议主要有以下的特点：

- 在网络中传递不经加密的用户名和口令 —— 许多旧有的协议，如 Telnet 和 FTP，都不会加密验证会话，应该尽可能地避免使用。
- 不经加密地在网络中传递保密信息 —— 许多协议在网络中不经加密地传递信息。这些协议包括 Telnet、FTP、HTTP、和 SMTP。许多网络文件系统，如 NFS 和 SMB，也不经加密地在网络中传递信息。在使用这些协议时，限制传输数据是用户的责任。

另外，像 netdump 之类的远程内存转储服务会把内存内容不经加密地在网络中传递。内存转储中可能包含口令，还可能包含数据库的数据和其它保密信息。

其它服务如 finger 和 rwhod 会揭示关于系统用户的信息。

带有固有不安全因素的服务包括：

- rlogin
- rsh
- telnet
- vsftpd

所有远程登录和 shell 程序（rlogin、rsh 和 telnet）都应该避免使用，使用 SSH 来替代它们。

FTP 的安全隐患没有远程 shel 那么严重，但是 FTP 服务器必须被谨慎配置和监视才能避免问题的发生。

应该谨慎实现并放置在防火墙之后的服务包括：

- finger
- identd

- netdump
- netdump-server
- nfs
- rwhod
- sendmail
- smb (Samba)
- yppasswdd
- ypserv
- ypxfrd

4.5.6 个人防火墙

配置了网络服务，设置防火墙是非常重要。

防火墙是防止网络分组进入系统的网络接口。如果某个被防火墙禁用的端口上接收到了一个请求，这个请求就会被忽略。如果某个服务在这些被禁用的端口之一监听请求，就不会收到任何分组，和禁用没什么区别。由于这个原因，应该小心谨慎，在配置防火墙禁用端口的同时不要禁用已配置服务正使用的端口。

对多数用户来说，配置简单防火墙的最佳工具是 GTES10 携带的简单的图形化防火墙配置工具：安全级别配置工具（system-config-securitylevel）。这个工具使用控制板界面为常规目的创建比较广义的 iptables 规则。

对于资深用户和服务器管理员来说，使用 iptables 来手工配置防火墙可能是最佳办法。

4.5.7 被安全强化的通信工具

随着互联网的发展和普及，劫获通信的可能性也随之增强。多年来，许多用于加密通过网络传输的通信的工具都被开发了出来。

GTES10 附带了两种使用基于公钥加密术的高级加密算式来保护正在通过网络传输的信息。

- OpenSSH —— 用于加密网络通信的 SSH 协议的免费实现。
- Gnu Privacy Guard (GPG) —— 用于加密数据的 PGP (Pretty Good Privacy) 加密程序的免费实现。

OpenSSH 是进入远程机器的安全方法，可以用来代替较老的 telnet 和 rsh 之类的不加密的服务。OpenSSH 包含一个叫做 sshd 的服务和三个命令行客户应用程序：

- ssh —— 一个安全远程控制台存取客户。
- scp —— 一个安全远程复制命令。
- sftp —— 一个允许不互动文件传输会话的伪 ftp 客户。

GPG 是保持私有数据隐蔽性的好办法。它可以被用来通过公共网络和电子邮件来发送保密数据，也可以被用来保护硬盘上的保密信息。

4.6 GTES10 服务器安全

当系统被用作公共网络的服务器时，它就会成为攻击对象。因此，对于系统管理员来说，加强系统防御和关闭某些服务就显得至关重要。

以下是用来增强服务器安全性的常识：

- 更新所有的服务来防御最新出现的威胁。
- 尽量使用安全协议。
- 在每台机器上尽量只使用一种网络服务的类型。
- 密切监视所有服务器上的可疑活动。

4.6.1 使用 TCP 会绕程序和 xinetd 来维护服务安全

TCP 会绕程序（TCP wrappers）为多项服务提供访问控制。多数现代的网

络服务，如 SSH、Telnet 和 FTP，都使用 TCP 会绕程序。该会绕程序位于进入请求和被请求服务之间。

当与 xinetd 一起使用时，TCP 会绕程序的优越性就更为显著。xinetd 是一种提供附加的访问、记录、关联、重导向和资源利用控制的超级服务。

以下各小节集中讨论特定的安全选项。

4.6.1.1 使用 TCP 会绕程序来强化安全

TCP 会绕程序的能力不仅仅局限于拒绝对服务的访问。本节说明如何使用它来发送连接横幅、警告来自特定主机的攻击、以及如何使用它来增强记录功能。

4.6.1.1.1 TCP 会绕程序和连接横幅

给连接服务的客户发送一幅警戒性横幅是掩盖服务器所使用的系统的好办法。要为某服务实现 TCP 会绕程序横幅，请使用 banner 选项。

这个例子为 vsftpd 实现了一个横幅。首先，创建一个横幅文件。它可以位于系统上的任何地方，但是它的名称必须和守护进程相同。在这个例子中，该文件叫做 /etc/banners/vsftpd。

该文件的内容如下所示：

```
220-Hello, %c

220-All activity on ftp.example.com is logged.

220-Act up and you will be banned.
```

%c 代符提供了各类客户信息，如用户名和主机名，或用户名和 IP 地址，从而使连接更令人生畏。

要把这个横幅展示给每个进入连接，把以下行添加到 /etc/hosts.allow 文件中：

```
vsftpd : ALL : banners /etc/banners/
```

4.6.1.1.2 TCP 会绕程序和攻击警告

如果发现某个主机或网络被正在攻击服务器，TCP 会绕程序可以通过 spawn 指令对来自该主机或网络的后续攻击向管理员发出警告。

在这个例子中，假定发现来自 206.182.68.0/24 网络的怪客正在试图攻击服务器。如果把以下行添加到 /etc/hosts.deny 文件中，连接企图就会被拒绝并记录在一个特殊的文件中。

```
ALL : 206.182.68.0 : spawn /bin/ 'date' %c %d >> /var/log/intruder_alert
```

%d 代符提供攻击者其它访问的服务名称。

要运行连接并记录日志，把 spawn 指令放在 /etc/hosts.allow 文件中。

4.6.1.1.3 TCP 会绕程序和强化记录告

如果某类连接比其它连接更值得关注，你可以通过 severity 选项来提高该类服务的记录级别。

在这个例子中，假定每个企图连接 FTP 服务器的端口 23（Telnet 端口）的客户都是怪客。在日志文件中放置一个 emerg 标记而不是使用默认的 info 标记来否定连接。

要达到这个目的，把以下行放在 /etc/hosts.deny 文件中：

```
in.telnetd : ALL : severity emerg
```

它使用默认的 authpriv 记录设施，但是把优先级别从默认的 info 提高到 emerg，这会把日志消息直接显示在控制台上。

4.6.1.2 使用 xinetd 来增强安全性

xinetd 超级服务器是另一个用来控制对其从属服务访问的有用工具。本节集中讨论如何使用 xinetd 来设置陷阱服务，以及如何使用它来控制任何给定 xinetd 服务可以使用的资源数量，从而阻挠拒绝服务攻击。

4.6.1.2.1 设置陷阱

xinetd 的一个重要功能是把主机添加到全局 no_access 列表的能力。如果一个主机在这个列表上，它对 xinetd 管理的服务的后续连接都会被拒绝一段时间，直到 xinetd 被重新启动为止。这是通过使用 SENSOR 属性来实现的。该技术是阻塞试图扫描服务器端口的主机的简单方法。

设置 SENSOR 的第一个步骤是选择禁止的服务。以下以 Telnet 为例进行说明。

编辑 /etc/xinetd.d/telnet 文件，把含有 flags 的行改成：

```
flags                  = SENSOR
```

在括号内添加以下行：

```
deny_time            = 30
```

这会拒绝试图连接到端口的主机在今后 30 分钟内的所有连接。deny_time 属性还有一个可接受的值是 FOREVER，它会使该禁令在 xinetd 被重新启动前保持有效；NEVER 则会允许连接并且记录它。

最后，确定一下这个文件的最后一行是：

```
disable                = no
```

虽然使用 SENSOR 是检测和阻止恶意主机和你的服务器建立连接的好办法。它有两个缺点：

- 它对暗中扫描不起作用。
- 知道 SENSOR 在运行的攻击者可以通过伪造 IP 地址和连接到禁用端口来对某些特定主机发起"拒绝服务"攻击。

4.6.1.2.2 控制服务器资源

xinetd 的另一个重要功能是它能够控制从属服务可以使用的资源量。

它通过以下指令来达到这个目的：

- cps = <number_of_connections> <wait_period> —— 指定每秒钟内被允许到服务的连接数量。该指令只接受整数值。
- instances = <number_of_connections> —— 指定允许到服务的连接总

数。该指令接受整数值或 UNLIMITED。

• per_source = <number_of_connections> —— 指定每个主机被允许到服务的连接数量。该指令接受整数值或 UNLIMITED。

• rlimit_as = <number[K|M]> —— 指定服务可以占用的内存地址空间数量，以千字节或兆字节为单位。该指令接受整数值或 UNLIMITED。

• rlimit_cpu = <number_of_seconds> —— 指定服务占用 CPU 的时间（以秒为单位）。该指令接受整数值或 UNLIMITED。

使用这些指令有助于防止某个 xinetd 服务大量占用系统，从而导致"拒绝服务"情况的出现。

4.6.2 保护 Portmap 的安全性

portmap 服务是用于 RPC 服务（如 NIS 和 NFS）的动态端口分配守护进程。它的验证机制比较薄弱，而且具备为它所控制的服务分配大范围端口的能力。由于这些原因，要保护它的安全比较困难。

如果运行 RPC 服务，请遵守以下基本规则。

4.6.2.1 使用 TCP 会绕程序来保护 portmap

使用 TCP 会绕程序来限制可以使用 portmap 服务的网络或主机这一点很重要，因为 portmap 没有内建的验证方式。

更进一步，在限制对服务的使用时，只使用 IP 地址。避免使用主机名，因为主机名可以通过 DNS 污染或其它方法被伪造。

4.6.2.2 使用 IPTables 来保护 portmap

要进一步限制对 portmap 服务的使用，在服务器上添加 IPTables 规则来限制对指定网络的访问是一个好办法。

以下是两个 IPTables 命令的例子: 只允许从网络 192.168.0/24 和本地主机（Nautilus 程序使用的 sgi_fam 服务所需要的）到 portmap 服务（监听

端口 111）的 TCP 连接。所有其它分组都被放弃。

```
iptables -A INPUT -p tcp -s! 192.168.0.0/24    --dport 111 -j DROP
iptables -A INPUT -p tcp -s 127.0.0.1    --dport 111 -j ACCEPT
```

要以相似的方法限制 UDP 连接，使用以下命令。

```
iptables -A INPUT -p udp -s! 192.168.0.0/24    --dport 111 -j DROP
```

4.6.3 保护 NIS 的安全

NIS 代表网络信息服务（Network Information Service）。它是叫做 ypserv 的 RPC 服务，和 portmap 以及其它相关服务一起使用，被用来为属于 NIS 域内的计算机间分发关于用户名、口令、以及其它保密信息的映射表。

NIS 服务器包括几个应用程序。它们是：

- /usr/sbin/rpc.yppasswdd —— 又称 yppasswdd 服务，该守护进程允许用户改变他们的 NIS 口令。
- /usr/sbin/rpc.ypxfrd —— 又称 ypxfrd 服务，该守护进程负责在网络上传输 NIS 映射表。
- /usr/sbin/yppush —— 该应用程序把 NIS 数据库的改变传播给多个 NIS 服务器。
- /usr/sbin/ypserv —— 这是 NIS 服务器守护进程。

按照今天的标准来看，NIS 不太安全。它没有主机验证机制，在网络上明文传输所有的信息，包括口令散列。因此，在设置使用 NIS 的网络时必须格外谨慎。默认的 NIS 配置就有其固有的不安全性。

4.6.3.1 谨慎制定网络计划

因为 NIS 在网络上明文传输保密信息，所以让服务器在防火墙背后的一个安全的网络段上运行就很重要。在不安全的网络上传递 NIS 信息都有被截取的危险。谨慎制定网络计划有助于防御严重的安全破坏。

4.6.3.2 使用像口令一样的 NIS 域名和主机名

NIS 域内的任何机器都不经验证就可以使用命令从服务器中抽取信息，只要用户知道 NIS 服务器的 DNS 主机名和 NIS 域名即可。

例如：如果某人把便携电脑连接到网络上，或从外部闯入了网络（而且成功地假冒了内部 IP 地址），以下命令会揭示 /etc/passwd 映射表：

```
ypcat -d <NIS_domain> -h <DNS_hostname> passwd
```

如果攻击者是一个根用户，他就可以通过键入以下命令来获得 /etc/shadow 文件：

```
ypcat -d <NIS_domain> -h <DNS_hostname> shadow
```

要使攻击者不能够轻易地获取 NIS 映射表，你可以为 DNS 主机名创建一个随机字符串，比如 o7hfawtgmhwg.domain.com。同理，你还可以创建一个不同的随机 NIS 域名。这就令攻击者进入 NIS 服务器比较困难。。

4.6.3.3 编辑 /var/yp/securenets 文件

如果 /var/yp/securenets 文件是空白的或不存在（默认方式安装），NIS 就会监听所有网络。你所要做的第一件事是在文件中放置一对子网掩码/网络值，因此 ypserv 只会对来自恰当网络的请求做出答复。

以下是 /var/yp/securenets 文件中的示例项目：

```
255.255.255.0        192.168.0.0
```

这种技术并不提供对 IP 假冒攻击的保护，但是它至少限制了 NIS 服务器要为哪些网络提供服务。

4.6.3.4 分配静态端口，使用 IPTables 规则

所有和 NIS 相关的服务器都可以被分配给指定的端口，只有 rpc.yppasswdd 例外 —— 该守护进程允许用户改变他们自己的登录口令。给其它两个 NIS 服务器守护进程，rpc.ypxfrd 和 ypserv 分配端口可以允

许管理员创建防火墙规则来进一步保护 NIS 服务器守护进程免受入侵。

要达到这个目的，把以下几行添加到 /etc/sysconfig/network 中：

```
YPSERV_ARGS="-p 834"
YPXFRD_ARGS="-p 835"
```

以下 IPTables 规则可以被用来实施服务器会监听哪些网络上的这些端口。

```
iptables -A INPUT -p ALL -s! 192.168.0.0/24   --dport 834 -j DROP
iptables -A INPUT -p ALL -s! 192.168.0.0/24   --dport 835 -j DROP
```

4.6.3.5 使用 Kerberos 验证

使用 NIS 验证的一个最明显的固有缺陷是，无论何时用户在机器上登录，/etc/shadow 映射表中的口令散列都会在网络上发送。如果入侵者获得了到 NIS 域的进入权，并且开始嗅探网络流量，他就可以悄悄地收集用户名和口令散列。只要有足够的时间，口令破译程序就可以猜出薄弱的口令，攻击者就可以获得对网络上有效帐号的使用权。

Kerberos 使用密钥加密技术，口令散列就决不会在网络上传送，从而使系统更加安全。

4.6.4 保护 NFS 的安全

网络文件系统或 NFS 是被用来为客户机器提供可联网存取的文件系统。

4.6.4.1 谨慎制定网络计划

现在 NFSv4 已经在网上传送使用 Kerberos 加密的信息，如果它是在防火墙背后或是在一个分段的网络上，谨慎配置这个服务是非常重要的。NFSv2 和 NFSv3 数据在网络上的传输仍是不安全的，在网络配置时需要把它考虑进去。谨慎制定网络计划有助于防御入侵。

4.6.4.2 注意语法错误

NFS 服务器通过/etc/exports 文件来决定要导出哪些文件系统，以及把这些目录导出到哪些主机上。编辑这个文件的时候要特别小心不要添加额外的空格。

例如：/etc/exports 文件中的以下行会令主机 bob.example.com 可以共享读写/tmp/nfs/ 目录。

```
/tmp/nfs/        bob.example.com(rw)
```

但是/etc/exports 中该行的情况却不同。它共享同一目录，让主机 bob.example.com 拥有只读权限，却给全局以读写权限。这全是由主机后面的一个空格造成的。

```
/tmp/nfs/        bob.example.com (rw)
```

通过使用 showmount 命令来校验哪些目录被共享，从而检查你的 NFS 共享配置是一个好习惯。

```
showmount -e <hostname>
```

4.6.4.3 不要使用 no_root_squash 选项

按照默认设置，NFS 共享把根用户改成用户 nfsnobody，它是一个不具备特权的用户帐号。这样，所有根用户创建的文件都会被用户 nfsnobody 所有，从而防止了设置了 setuid 的程序被上传到系统。

如果使用了 no_root_squash，远程根用户就能够改变共享文件系统上的任何文件，从而可以使设置了特洛伊木马的程序被执行。

4.6.5 保护 Apache HTTP 服务器的安全

Apache HTTP 服务器是 GTES10 包括的最稳定和最安全的服务之一。保护 Apache HTTP 服务器安全的方法和技术很多 —— 在这里我们无法逐一详述。

以下是管理员应该小心使用的配置选项列表。

4.6.5.1 FollowSymLinks

该指令被默认启用,在创建到万维网服务器的文档根的符号链接时请小心。例如，提供一个到 / 的符号链接就不是个好主意。

4.6.5.2 Indexes 指令

该指令被默认启用，但它可能不应该被启用。要阻止访问者浏览服务器上的文件，你可以删除该指令。

4.6.5.3 UserDir 指令

UserDir 指令被默认禁用，因为它可以确认某个用户帐号在系统上是否存在。要启用服务器上的用户目录浏览，请使用以下指令：

```
UserDir enabled
UserDir disabled root
```

这些指令为除了 /root/ 以外的所有用户目录激活浏览。要把用户添加到禁用帐号列表中，在 UserDir disabled 行中添加一个用空格隔开的用户列表。

4.6.5.4 不要删除 IncludesNoExec 指令

按照默认设置，服务器端包括（server-side includes）模块不能执行命令。除非在极端必要的情况下，建议你不要改变这个设置，因为它有可能会使攻击者能够在系统上执行命令。

4.6.5.5 限制对可执行目录的权限

对于任何包含脚本或 CGI 的目录，请确定只给根用户以写权限。这可以通过键入以下命令来达到：

```
chown root <directory_name>chmod 755 <directory_name>
```

还有，一定要在脚本实际使用之前校验它们在系统上的运行情况是否正确。

4.6.6 保护 FTP 的安全

文件传输协议（FTP）是用来在网络上传输文件的早期 TCP 协议。因为所有服务器的事务，包括用户验证，都是不经加密的，所以它也被认为是不安全的协议，应该谨慎配置。

GTES10 提供三种 FTP 服务器。

- gssftpd —— 使用了 Kerberos 的，基于 xinetd 的 FTP 守护进程。它不在网络中传递验证信息。
- 内容加速器（tux）—— 带有 FTP 能力的内核空间万维网服务器。
- vsftpd —— 一个独立的面向安全的 FTP 服务。

以下保安原则适用于设置 vsftpd FTP 服务。

4.6.6.1 FTP 问候横幅

在提供用户名和口令前，所有的用户都会看到一个问候横幅。按照默认设置，该横幅含有版本信息，这有利于怪客找出系统的漏洞。

要改变 vsftpd 的问候横幅，把以下指令添加到 /etc/vsftpd/vsftpd.conf 中：

```
ftpd_banner=<insert_greeting_here>
```

把以上指令中的 <insert_greeting_here> 替换成问候消息。

对于多行横幅，你最好是使用一个横幅文件。要简化对多个横幅的管理，把所有横幅都放在一个叫做 /etc/banners/ 的新目录中。在这个例子中，FTP 连接的横幅文件是 /etc/banners/ftp.msg。以下是这类文件的例子：

```
######################################################
Hello, all activity on ftp.example.com is logged.
######################################################
```

要为 vsftpd 引用这个问候横幅文件，把以下指令添加到

/etc/vsftpd/vsftpd.conf 中：

```
banner_file=/etc/banners/ftp.msg
```

你还可以使用 TCP 会绕程序给进入连接发送附加横幅。

4.6.6.2 匿名访问

/var/ftp/ 目录的存在会激活匿名帐号。

创建这个目录的最简单方法是安装 vsftpd 软件包。该软件包会为匿名用户设置目录树并把目录的权限为匿名用户配置为只读。

按照默认设置，匿名用户不能对任何目录进行写操作。

要允许匿名用户上传文件，推荐你在 /var/ftp/pub/ 内创建只写目录。

按一下步骤，首先键入：

```
mkdir /var/ftp/pub/upload
```

下一步，改变权限使匿名用户看不到目录中的内容，键入：

```
chmod 730 /var/ftp/pub/upload
```

长格式的目录列表看起来应该像：

```
drwx-wx---    2 root    ftp        4096 Feb 13 20:05 upload
```

此外，在 vsftpd 下添加以下一行/etc/vsftpd /vsftpd.conf 到文件中：

```
anon_upload_enable=YES
```

4.6.6.3 用户帐号

因为 FTP 在不安全的网络中传递明文用户名和口令来验证，拒绝系统用户从他们的用户帐号来进入服务器是一个好办法。

要在 vsftpd 中禁用用户帐号，在 /etc/vsftpd/vsftpd.conf 中添加以下指令：

```
local_enable=NO
```

禁用某组特定帐号（如根用户帐号，以及有 sudo 特权的用户帐号）的最

简单方法是使用 PAM 列表文件。vsftpd 的 PAM 配置文件是/etc/pam.d/vsftpd。

你还可以在每个服务中直接禁用用户帐号。

要在 vsftpd 中禁用指定用户帐号，把用户名添加到/etc/vsftpd.ftpusers 中。

4.6.6.4 使用 TCP 会绕程序来控制访问

使用 TCP 会绕程序来控制到每种 FTP 守护进程的访问。

4.6.7 保护 Sendmail 的安全

Sendmail 是使用简单邮件传输协议（SMTP）的邮件传输代理（MTA）。它在其它 MTA 和电子邮件客户或分发代理之间传送电子消息。虽然一些 MTA 能够加密彼此间的通信，但多数却不能，因此通过公共网络发送邮件被认为是一种带有固有不安全因素的通信方式。

配置 Sendmail 服务器需要考虑以下问题。

4.6.7.1 限制"拒绝服务"攻击

由于电子邮件的性质，一个攻击者可以轻易地使用邮件来极大地增加服务器的系统开销，从而导致拒绝服务的攻击。通过设置/etc/mail/sendmail.mc 的以下目录的限度，这类攻击的有效性就会大受限制。

- confCONNECTION_RATE_THROTTLE —— 服务器每秒能够接受的连接数量。按照默认设置，Sendmail 不限制连接数量。如果限度被设置并到达，以后的连接就会被延迟。
- confMAX_DAEMON_CHILDREN —— 服务器能够分出的子进程的最大数量。按照默认设置，Sendmail 不限制子进程的数量。如果限度被设置并达到，以后的连接就会被延迟。
- confMIN_FREE_BLOCKS —— 必须为服务器保留的用来接受邮件的空闲块的最少数量。默认为 100 块。

- confMAX_HEADERS_LENGTH —— 消息头的可接受大小的最大限度（以字节为单位）。
- confMAX_MESSAGE_SIZE —— 单个消息的可接受大小的最大限度（以字节为单位）。

4.6.7.2 NFS 和 Sendmail

不要把邮件假脱机目录/var/spool/mail/ 放在 NFS 共享文件卷上。

在 NFSv2 和 NFSv3 中，系统对用户组群 ID 没有控制。因此，几个 UID 相同的用户可以收到和阅读彼此的邮件。NFSv4 使用 Kerberos 而不是使用基于 UID 的用户认证。所以在 NFSv4 中就不会出现这种情况。

4.6.7.3 只使用电子邮件程序访问 Sendmail 服务器

要防止本地用户利用 Sendmail 服务器上的漏洞，最好是让邮件用户只使用电子邮件程序来访问 Sendmail 服务器。邮件服务器上的 Shell 帐号不应该被允许，/etc/passwd 文件中的所有用户 shell 都应该被设置为 /sbin/nologin（根用户可能是个例外）。

4.6.8 校验哪些端口正在监听

配置了网络服务之后，关注一下哪些端口在监听系统的网络接口这一点很重要。任何打开的端口都可能会是网络正被入侵的证明。

要列举正在监听网络的端口，有两种基本方法。一种不太可靠的方法是通过键入 netstat -an 或 lsof -i 之类的命令来查询网络堆栈。这种方法之所以不太可靠是因为这些程序不连接网络上的机器，而是查看系统上在运行什么。因此，它们频繁成为攻击者的替换目标。怪客在打开了未经授权的网络端口后，就以这种方法来企图掩盖他们的踪迹。

更可靠的方法是使用 nmap 之类的端口扫描器来检查哪些端口正在监听网络。

以下从控制台发出的命令会判定哪些端口在监听来自网络上的 TCP 连接：

```
nmap -sT -O localhost
```

该命令的输出和以下相似：

```
Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-09-24 13:49 EDT
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind
113/tcp   open  auth
631/tcp   open  ipp
834/tcp   open  unknown
2601/tcp  open  zebra
32774/tcp open  sometimes-rpc11
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 12.857 days (since Sat Sep 11 17:16:20 2004)
Nmap run completed -- 1 IP address (1 host up) scanned in 5.190 seconds
```

该输出显示了由于 sunrpc 服务的存在，系统正在运行 portmap。然而，端口 834 上还有一个神秘服务。要查看一下该端口是否和任何已知服务相关，键入：

```
cat /etc/services | grep 834
```

该命令没有返回任何输出。这表明虽然该端口是在保留范围内（即从 0 到 1023 内），并且需要根权限才能打开，它并没有关联任何已知服务。

下一步，检查使用 netstat 或 lsof 的端口的信息。要使用 netstat 检查端口 834，使用以下命令：

```
netstat -anp | grep 834
```

该命令返回以下输出：

```
tcp    0    0 0.0.0.0:834    0.0.0.0:*    LISTEN    653/ypbind
```

这个开放端口在 netstat 中存在，这一点比较令人放心，因为如果怪客在被攻击的系统上暗中打开一个端口，他们很可能不会让这个端口使用该命令被暴露出来。还有，[p] 选项揭示了打开这个端口的进程 id（PID）。在这个例子中，被打开的端口属于 ypbind（NIS），这是和 portmap 服务一起进行的 RPC 服务。

lsof 命令揭示了相似的信息，因为它也能够链接开放端口和服务：

```
lsof -i | grep 834
```

以下是这个命令中和讨论有关的输出部分：

```
ypbind    653    0    7u    IPv4    1319    TCP *:834 (LISTEN)
ypbind    655    0    7u    IPv4    1319    TCP *:834 (LISTEN)
ypbind    656    0    7u    IPv4    1319    TCP *:834 (LISTEN)
ypbind    657    0    7u    IPv4    1319    TCP *:834 (LISTEN)
```

这些工具揭示了大量关于运行在机器上的服务状态的信息。它们很灵活，能够提供关于网络服务和配置的许多信息。强烈推荐你阅读 lsof、netstat、nmap 和 services 的说明书页。

4.7 虚拟专用网

带有卫星办公室的机构为了高效率和保护所传输机密数据的安全性而经常使用专用线路来彼此连接。例如，许多公司使用帧中继或不对称传输模式

（Asynchronous Transfer Mode，ATM）线路作为连接办公室的端点到端点的解决方案。这种方法比较昂贵，特别对于想要扩展而又想避免企业级别的专用数字线路带来的昂贵支出的中小型企业而言。

为满足这种需要，虚拟专用网（Virtual Private Networks，VPN）由此而被开发而出。VPN 使用和专用线路相同的原理，它允许在两个节点（或网络）间进行安全的数字通信，从现存的本地网（Local Area Networks，LAN）中创建一个广域网（WAN）。它和帧中继或 ATM 的不同之处在于所用的传输介质。VPN 使用数据报（UDP）作为传输层，但通过 IP 来传输，把它变成一个到目标点的安全通道。多数免费的软件 VPN 实现包括了开放标准、开源加密来进一步掩护传输中的数据。

某些组织使用硬件 VPN 来进行保护，而有些组织使用软件或基于协议的实现方法。Cisco、Nortel、IBM 和 Checkpoint 等几家厂商提供了硬件 VPN 解决方案。有一种叫做 FreeS/Wan 的用在 Linux 上的基于软件的免费 VPN 解决方案，它利用了标准化的 IPsec 实现措施。这些 VPN 解决方案充当位于办公室和办公室之间的 IP 连接的特殊路由器。

当分组从客户中被传输，它通过路由器或网关被发送，然后在其中添加叫做验证头（Authentication Header，AH）的关于选路和验证的头信息。该数据是被加密的，并且被包含在叫做封装安全载荷（Encapsulating Security Payload，ESP）的解密和处理说明中。接收 VPN 路由器会剥离头信息，把它选路发送到所要去的目的地（工作站或网络上的节点）。网络到网络间 VPN 连接的加密和解密进程对本地节点是透明的。

使用了这种被提高了的安全级别，怪客不但必须劫获分组，还需要能够解密分组。利用客户和服务器间的中间人攻击方法的入侵者还必须获取用于验证会话的钥匙。因为 VPN 使用多层次的验证和加密，因此它是把多个远程节点连接成一个统一的内联网的安全而有效的方法。

4.7.1 VPN 和 GTES10

GTES10 用户在实施软件解决方案来安全地连接 WAN 方面有很多选择。"互联网协议安全"（Internet Protocol Security），又称 IPsec，是被 GTES10

支持的实现方式。它充分满足了带有分支办公室或远程用户的机构的使用需要。

4.7.2 IPsec

GTES10 支持使用 IPsec 在公共载体网络（如互联网）上使用安全隧道来连接远程主机和网络。IPsec 可以使用主机到主机或网络到网络（一个 LAN/WAN 到另一个 LAN/WAN）来实现。GTES10 中的 IPsec 实现使用互联网密钥交换（Internet Key Exchange，IKE）。它是一个被互联网工程任务组（Internet Engineering Task Force，IETF）实现的用于彼此验证和安全连接系统的协议。

IPsec 连接被分成两个逻辑阶段。在第一阶段，IPsec 节点引发和远程节点或网络的连接。远程节点或网络检查请求节点的证件，双方商谈连接所用的验证方法。在 GTES10 系统上，IPsec 连接使用 IPsec 节点验证的"预共享钥匙"（pre-shared key）方法。在预共享钥匙 IPsec 连接中，双方主机必须使用同一钥匙才能进入 IPsec 连接的第二阶段。

IPsec 连接的第二阶段在 IPsec 节点间创建"安全关联"（security association，SA）。该阶段使用配置信息（如加密方法、密钥互换参数等等）来建立 SA 数据库。它管理远程节点和网络间的实际 IPsec 连接。

GTES10 中的 IPsec 实现使用 IKE 来在互联网的主机间共享钥匙。racoon 这个钥匙守护进程处理 IKE 钥匙分发和交换任务。

4.7.3 IPsec 安装

实现 IPsec 要求你在所有 IPsec 主机（若使用主机到主机配置）或路由器（若使用网络到网络配置）上安装 ipsec-tools RPM 软件包。RPM 软件包中包含帮助你设置 IPsec 连接所必需的库、守护进程和配置文件。

- /lib/libipsec.so —— 包含 GTES10 中使用的 Linux 内核与 IPsec 实现间的 PF_KEY 信任的钥匙管理套接字接口。
- /sbin/setkey —— 在内核中操作 IPsec 的钥匙管理和安全属性。该可执

行文件被 racoon 钥匙管理守护进程控制。

• /sbin/racoon —— IKE 钥匙管理守护进程，用来管理和控制 IPsec 连接的系统之间的安全关联和钥匙共享。守护进程可以通过编辑 /etc/racoon/racoon.conf 文件而被控制。

• /etc/racoon/racoon.conf —— racoon 守护进程配置文件，用来配置 IPsec 连接的各个方面，包括连接中使用的验证方法和加密算式。

在 GTES10 上配置 IPsec 可以通过网络管理工具来进行，也可以通过手工编辑联网和 IPsec 配置文件来进行。

4.7.4 IPsec 主机到主机配置

创建连接的第一步是从每个工作站收集系统和网络信息。对于主机到主机连接，你需要以下信息：

• 两个主机的 IP 地址

• 用来把 IPsec 连接从其它设备或连接中区别出来的独特名称（如 ipsec0）

• 固定的加密钥匙或被 racoon 自动生成的钥匙

• 被用来初始连接和在会话中交换加密钥匙的预共享验证钥匙

例如：假定工作站 A 和工作站 B 想通过 IPsec 隧道来彼此连接。它们想使用值为 foobarbaz 的预共享钥匙来连接，并且用户同意让 racoon 自动生成和共享每个主机间的验证钥匙。两个主机用户都决定把它们的连接命名为 ipsec0。

以下是工作站 A 和工作站 B 之间的主机到主机 IPsec 连接的 ifcfg 文件（这个例子中用来识别该连接的独特名称是 ipsec0，因此其结果文件被命名为/etc/sysconfig/network-scripts/ifcfg-ipsec0）。

```
DST = x.x.x.x

TYPE = IPSEC

ONBOOT=yes
```

```
IKE_METHOD=PSK
```

工作站 A 将会把 X.X.X.X 替换成工作站 B 的 IP 地址，而工作站 B 将会把 X.X.X.X 替换成工作站 A 的 IP 地址。连接被设置成引导时被引发（ONBOOT=yes），并使用预共享钥匙验证方法（IKE_METHOD=PSK）。

以下是预共享钥匙文件（叫做 /etc/sysconfig/network-scripts/keys-ipsec0），两个工作站都使用它来彼此验证。该文件的内容应该完全一致，并且只有根用户才应该有读写权。

```
IKE_PSK=foobarbaz
```

如果需要改变验证钥匙，必须编辑两个工作站上的 keys-ipsec0 文件。两个文件必须完全一致才能保证正确的连接性。

下一个例子显示了到远程主机的第一阶段连接的特有配置。该文件的名称为 X.X.X.X.conf（把 X.X.X.X 替换成远程 IPsec 路由器的 IP 地址）。注意，一旦 IPsec 隧道被激活，该文件会被自动生成，不应该被直接编辑。

```
;
remote X.X.X.X
{
        exchange_mode aggressive, main;
        my_identifier address;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
               dh_group 2 ;
        }
}
```

默认的第一阶段配置文件在 IPsec 连接被引发时被创建。它包含以下

GTES10 的 IPsec 实现所使用的声明：

- remote X.X.X.X

指明随后的配置文件实例只应用于被 X.X.X.X IP 地址所识别的远程节点。

- exchange_mode aggressive

在 GTES10 中，IPsec 的默认配置使用强硬的验证模式。这种模式减少连接费用，同时允许到多个主机的多个 IPsec 配置。

- my_identifier address

定义验证节点时要使用的身份识别方法。GTES10 使用 IP 地址来识别节点。

- encryption_algorithm 3des

定义验证时使用的加密术。默认使用"三次数据加密标准"（Triple Data Encryption Standard，3DES）。

- hash_algorithm sha1

指定在节点商谈过程的第一阶段中使用的散列算式。默认使用安全散列算式（Secure Hash Algorithm）版本 1。

- authentication_method pre_shared_key

定义节点商谈中使用的验证方法。GTES10 默认使用预共享钥匙。

- dh_group 2

指定建立动态生成的会话钥匙所用的 Diffie-Hellman 组号。默认使用 1024 位组

除了 include "/etc/racoon/X.X.X.X.conf" 这个声明外，/etc/racoon/racoon.conf 文件应该完全一致。该声明（以及它引用的文件）在 IPsec 隧道被激活时被生成。对于工作站 A，include 声明中的 X.X.X.X 是工作站 B 的 IP 地址。工作站 B 的情况正好相反。下面显示了一个当 IPsec 连接被激活时的典型 racoon.conf 文件。

```
# Racoon IKE daemon configuration file
```

```
.# See 'man racoon.conf' for a description of the format and entries.
path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";
sainfo anonymous
{
        pfs_group 2;
        lifetime time 1 hour ;
        encryption_algorithm 3des, blowfish 448, rijndael ;
        authentication_algorithm hmac_sha1, hmac_md5 ;
        compression_algorithm deflate ;
}
include "/etc/racoon/X.X.X.X.conf"
```

默认的 racoon.conf 文件包含 IPsec 配置的指定路径，预共享钥匙和证书。sainfo anonymous 中的字段描述 IPsec 节点安全验证的第二阶段 ——IPsec 连接的性质（包括所用的被支持加密算式）和交换钥匙的方法。以下列表定义了第二阶段的字段：

- sainfo anonymous

意思是只要 IPsec 证件匹配，SA 能够不具名地引发和任何对端的连接。

- pfs_group 2

定义 Diffie-Hellman 钥匙交换协议。该协议会决定 IPsec 节点为 IPsec 连接的第二阶段建立彼此使用的临时会话钥匙的方法。GTES10 中实现的 IPsec 默认使用 Diffie-Hellman 加密术钥匙交换的组 2（或 modp1024）。组 2 使用 1024 位模块化取幂。这种方法在密钥被窃取时也能够防止攻击者解密前一次 IPsec 传输。

- lifetime time 1 hour

这个参数表明 SA 的整个过程可以使用时间或数据字节数量来衡量。GTES10 实现的 IPsec 指定了 SA 的生存期为 1 小时。

- encryption_algorithm 3des, blowfish 448, rijndael

指定第二阶段中所用的被支持的加密术。GTES10 支持 3DES、448 位 Blowfish、以及 Rijndael（用于"高级加密标准"（Advanced Encryption Standard，AES）中的加密术。

- authentication_algorithm hmac_sha1, hmac_md5

列举被支持的用来验证的散列算式。被支持的模式是 sha1 和 md5 散列消息验证代码（hashed message authentication codes，HMAC）。

- compression_algorithm deflate

定义用于 IP 载量压缩（IPCOMP）支持的压缩算法。它具备在较慢的连接中较快地传输 IP 数据报的潜力。

要启动连接，在每个主机上以根用户身份重新引导工作站或执行以下命令：

```
/sbin/ifup ipsec0
```

要测试 IPsec 连接，运行 tcpdump 工具来查看在主机（或网络）间传输的网络分组，并校验它们是否通过 IPsec 被加密了。分组应该包括 AH 头，而且应该被显示为 ESP 分组。ESP 意味着它被加密了。例如：

```
17:13:20.617872 pinky.example.com > ijin.example.com: \

AH(spi=0x0aaa749f,seq=0x335): ESP(spi=0x0ec0441e,seq=0x335) (DF)
```

4.7.5 IPsec 网络到网络配置

IPsec 还可以使用网络到网络连接配置把整个网络（如 LAN 或 WAN）连接到一个远程网络上。网络到网络配置要求你在所连接网络的每一方设置 IPsec 路由器来处理和选路发送从一个网络上的节点到另一个远程网络上的节点间的信息。图 4-4 显示了一个网络到网络的 IPsec 隧道连接。

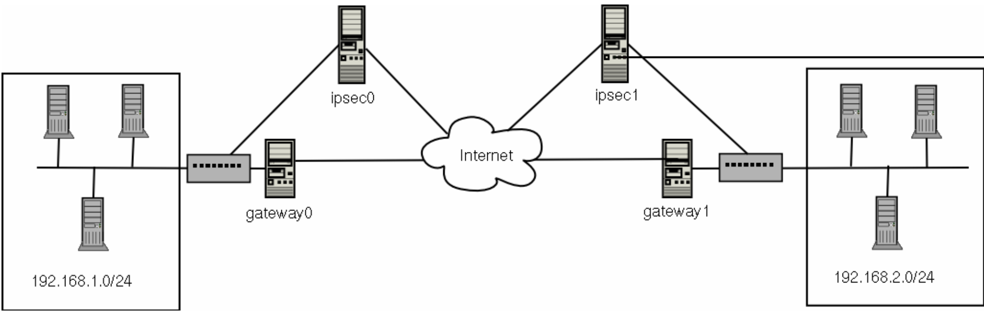


图 4-4 网络到网络的 IPsec 隧道连接

该图表显示了两个被互联网分开的 LAN。这些网络使用 IPsec 路由器来验证和引发使用通过互联网的安全隧道的连接。在传输中被劫获的分组需要强力解密才能攻破保护这些 LAN 之间的分组的加密。从 192.168.1.0/24 IP 范围的一个节点到 192.168.2.0/24 上的另一个节点间的通信对于这些节点而言是完全透明的，因为对 IPsec 分组的处理、加密、解密、以及选路都是由 IPsec 路由器完成。

网络到网络连接所需的信息包括：

- 专用 IPsec 路由器的可从外部进入的 IP 地址
- 被 IPsec 路由器提供服务的 LAN/WAN 的网络地址范围（如 192.168.0.0/24 或 10.0.1.0/24）
- 把来自网络节点的数据选路发送到互联网的网关设备的 IP 地址
- 用来把 IPsec 连接从其它设备或连接中区别出来的独特名称（如 ipsec0）
- 固定的加密钥匙或被 racoon 自动生成的钥匙
- 用来引发连接和在会话中交换加密钥匙的预共享验证钥匙

例如：假设 LAN A（lana.example.com）和 LAN B（lanb.example.com）想通过 IPsec 隧道来彼此连接。LAN A 的网络地址在 192.168.1.0/24 范围内，LAN B 使用 192.168.2.0/24 范围。LAN A 的网关 IP 地址是 192.168.1.254，LAN B 的网关地址是 192.168.2.254。IPsec 路由器不同于每个 LAN 的网关，并且使用两个网络设备：eth0 被分派给可从外部进入

的静态 IP 地址，它被用来进入互联网；eth1 充当在每个节点间和 eth0 设备中处理和传输 LAN 分组以便传输到互联网的选路点。

每个网络间的 IPsec 连接使用一个值为 GTES10 l1nux 的预共享钥匙，A 和 B 的管理员都同意让 racoon 自动生成和共享每个 IPsec 路由器之间的验证钥匙。LAN A 的管理员决定把 IPsec 连接命名为 ipsec0，而 LAN B 的管理员决定把 IPsec 连接命名为 ipsec1。

以下是 LAN A 的网络到网络 IPsec 连接的 ifcfg 文件。在这个例子中用来识别该连接的独特名称是 ipsec1，因此其结果文件被命名为 /etc/sysconfig/network-scripts/ifcfg-ipsec1.

```
TYPE=IPSEC

ONBOOT=yes

IKE_METHOD=PSK

SRCGW=192.168.1.254

DSTGW=192.168.2.254

SRCNET=192.168.1.0/24

DSTNET=192.168.2.0/24

DST=X.X.X.X
```

连接被设置成引导时被引发（ONBOOT=yes），并使用预共享钥匙验证方法（IKE_METHOD=PSK）。LAN A 的管理员输入目标网关（即 LAN B 的网关 DSTGW=192.168.2.254），以及源网关（即 LAN A 的网关 IP 地址 SRCGW=192.168.1.254）。然后，管理员输入目标网络，即 LAN B 的网络范围（DSTNET=192.168.2.0/24），以及源网络（SRCNET=192.168.1.0/24）。最后，管理员输入目标 IP 地址，它是 LAN B 的可从外界进入的 IP 地址（X.X.X.X）。

以下是预共享钥匙文件（叫做 /etc/sysconfig/network-scripts/keys-ipsecX，这里的 X 对 LAN A 来说是 0，对 LAN B 来说是 1），两个工作站都使用它来彼此验证。该文件的内容应该完全一致，并且只有根用户才应该有读写权。

```
IKE_PSK=GTES10 l1nux
```

如果需要改变验证钥匙，必须编辑两个 IPsec 路由器上的 keys-ipsecX 文件。这两个钥匙必须完全一致才能保证正确的连接性。

以下是 IPsec 连接的 /etc/racoon/racoon.conf 配置文件。注意，文件底部的 include 行只有在连接到 IPsec 隧道时才会出现，因为它是在 IPsec 连接被激活时被自动生成的。

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format and entries.
path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";
sainfo anonymous
{
        pfs_group 2;
        lifetime time 1 hour ;
        encryption_algorithm 3des, blowfish 448, rijndael ;
        authentication_algorithm hmac_sha1, hmac_md5 ;
        compression_algorithm deflate ;
}
include "/etc/racoon/X.X.X.X.conf"
```

以下是连接到远程网络的配置文件。该文件的名称为 X.X.X.X.conf（把 X.X.X.X 替换成远程 IPsec 路由器的 IP 地址）。注意，一旦 IPsec 隧道被激活，该文件会被自动生成。

```
;
remote X.X.X.X
{
```

```
        exchange_mode aggressive, main;
        my_identifier address;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2 ;
        }
}
```

在启动 IPsec 连接前，内核中应该启用 IP 转发。在 shell 提示下作为根用户来启用 IP 转发：

1. 编辑 /etc/sysctl.conf，把 net.ipv4.ip_forward 设置为 1。

2. 执行以下命令来启用改变：

```
sysctl -p /etc/sysctl.conf
```

要启动 IPsec 连接，重新引导 IPsec 路由器或在每个路由器上以根用户身份执行以下命令：

```
/sbin/ifup ipsec0
```

连接被激活，LAN A 和 LAN B 能够彼此通信。通过对 IPsec 连接运行 ifup，路线会通过初始脚本被自动创建。要显示网络的路线列表，运行以下命令：

```
/sbin/ip route list
```

要测试 IPsec 连接，运行 tcpdump 工具来查看在主机（或网络）间传输的网络分组，并校验它们是否通过 IPsec 被加密了。分组应该包括 AH 头，而且应该被显示为 ESP 分组。ESP 意味着它被加密了。例如，要检查 LAN A 的 IPsec 连接，键入：

```
tcpdump -n -i eth0 host lana.example.com
```

分组应该包含 AH 头，应该为显示为 ESP 分组。ESP 意味着它被加密了。例如（反斜线代表应该在一行上继续）：

```
12:24:26.155529 lanb.example.com > lana.example.com: \
        AH(spi=0x021c9834,seq=0x358): \
        lanb.example.com > lana.example.com:\
        ESP(spi=0x00c887ad,seq=0x358) (DF)    (ipip-proto-4)
```

4.8 防火墙

信息安全通常被当作一种不断改进的过程而不是一成不变的产品。然而，标准的安全实现通常会使用某种专用机制来控制存取权限；把对网络资源的使用限制在授权的、可识别身份的、和可追踪的用户范围内。GTES10 包括了好几种强大的工具来协助管理员和安全工程师们解决网络级别的存取控制问题。

除了 IPsec 之类的 VPN 解决方案外，防火墙是网络安全系统的一个重要组成部分。好几家推广防火墙方案的厂商都提供了满足各级市场需求的产品：从保护一台电脑的家庭用户的需求，到保护重要企业信息的数据中心方案。防火墙可以是单独的硬件解决方案，如 Cisco、Nokia、和 Sonicwall 的防火墙设备。Checkpoint、McAfee、以及 Symantec 等厂商还开发了家用和商用的专有软件防火墙解决方案。

除了硬件防火墙和软件防火墙间的区别外，各个防火墙在功能用途方面也有所区别。表 4-2 详细描述了三种常见的防火墙，以及它们的运行方式：

方法	描述	优越性	不利因素
NAT	网络地址转换(NAT)把内部网络的 IP 子网放置在一个或一组外部 IP 地址之后，把所	可以在 LAN 机器上被透明配置 保护在一个或多个外部 IP 地址之后的许多机器，简化管理任务	一旦用户从防火墙外连接了服务，则无法防止其蓄意活动

	有的请求都伪装成来自一个地址而不是多个不同地址。	用户到 LAN 的出入可以通过打开和关闭 NAT 防火墙/网关上的端口来限制	
分组过滤器	分组过滤防火墙读取每个进出 LAN 的数据分组。它可以根据头信息来读取和处理分组，并根据被防火墙管理员实施的可编排的规则来过滤分组。Linux 内核通过 Netfilter 内核子系统内建了分组过滤功能。	可以通过 iptables 这个前端工具而被定制 不需要任何客户方面的定制，因为所有的网络活动都在路由器级别而不是应用程序级别被过滤 由于分组没有通过代理来传输，客户和远程主机间是直接连接，因此网络传输速度比较快	无法像代理防火墙一样根据内容过滤分组 在协议层处理分组，但是无法在应用程序层处理分组 复杂的网络体系可能会使建立分组过滤规则方面比较困难，特别是在和 IP 伪装（IP masquerading）或本地子网及 DMZ 网络一起使用时
代理	代理防火墙过滤所有从 LAN 客户到代理机器的某种特定协议或类型的请求，然后，它再代表这个本地客户向互联网发送这些请求。代理机器被用来充当企图不良的远程用	使管理员拥有对 LAN 之外的应用程序和协议功能的控制权 某些代理服务器可以缓存数据，因此当客户存取频繁请求的数据时，这些数据就可以从本地缓存调出而不必使用互联网连接，这有助于减少不必要的带宽	代理通常是应用程序特有的（HTTP、Telnet 等）或在协议方面有限制的（多数代理只能用于 TCP 连接的服务） 应用程序服务无法在代理后面运行，因此你的应用程序服务器必须使用另一种网络保安措施

	户和内部网络客户机器之间的一个缓冲。	用量 代理服务可以被密切地监视和记录，从而允许你在网络资源用量方面有更严格的控制	代理可能会成为网络的瓶颈，因为所有的请求和传输都要经过一个中介而不是让客户直接连接远程服务

表 4-2. 防火墙类型

4.8.1 Netfilter 和 iptables

Linux 内核中有一个功能强大的联网子系统 Netfilter。Netfilter 子系统提供了有状态的或无状态的分组过滤，还提供了 NAT 和 IP 伪装服务。Netfilter 还具备为高级选路和连接状态管理而变形（mangle）IP 头信息的能力。Netfilter 是通过 IPTables 工具来控制的。

Netfilter 的强大功能和灵活性是通过 iptables 界面来实现的。这个命令行工具和它的前身 ipchains 的语法很相似；不过，iptables 使用 Netfilter 子系统来增进网络连接、检验、和处理方面的能力；ipchains 使用错综复杂的规则集合来过滤源地和目的地路线以及两者的连接端口。iptables 只在一个命令行界面中就包括了更先进的记录方式；选路前和选路后的行动；网络地址转换；以及端口转发。

4.8.2 使用 iptables

使用 iptables 的第一步是启动 iptables 服务。这可以使用以下命令进行：

```
service iptables start
```

要使 iptables 在系统引导时默认启动，你必须使用 chkconfig 来改变服务的运行级别状态。

```
chkconfig --level 345 iptables on
```

iptables 的语法被分成几个层次。主要层次为"链"（chain）。"链"指定处理

分组的状态。其用法为：

```
iptables -A chain -j target
```

-A 在现存的规则集合内后补一条规则。chain 是规则所在"链"的名称。iptables 中有三个内建的链（即影响每一个在网络中经过的分组的链）：INPUT、OUTPUT、和 FORWARD。这些链是永久性的，不能被删除。-j target 选项指定 iptables 应该"跳"（jump）到规则集中的哪条规则。内建的目标有：ACCEPT、DROP、和 REJECT。

-N 选项可以被用来创建新链（又称用户定义链）。创建新链在定制详尽或复杂规则方面很有用。

4.8.2.1 基本防火墙策略

初始建立的某些基本策略为建构更详细的用户定义的规则奠定了基础。iptables 使用策略（policy, -P）来创建默认规则。对安全敏感的管理员通常想采取丢弃所有分组的策略，只逐一允许指定分组。以下规则阻塞网络上所有的出入分组。

```
iptables -P INPUT DROP

iptables -P OUTPUT DROP
```

此外，还推荐你拒绝所有转发分组（forwarded packets） —— 要从防火墙被选路发送到它的目标节点的网络交通 —— 以便限制内部客户对互联网的无意暴露。要达到这个目的，使用以下规则：

```
iptables -P FORWARD DROP
```

设置了策略链后，为你的特定网络和安全需要创建新规则。以下各节概述了一些你在建构 iptables 防火墙时可能要实现的规则。

4.8.2.2 保存和恢复 iptables 规则

防火墙规则只在计算机处于开启状态时才有效。如果系统被重新引导，这些规则就会自动被清除并重设。要保存规则以便今后载入，请使用以下命令：

```
/sbin/service iptables save
```

保存在 /etc/sysconfig/iptables 文件中的规则会在服务启动或重新启动时（包括机器被重新引导时）被应用。

4.8.3 常用 iptables 过滤

把远程攻击者拒之"LAN"外是保护网络安全的最重要的一个方面。LAN 的完好性应该通过使用严格的防火墙规则抵御恶意的远程用户来保护。但是，如果默认策略被设置为阻塞所有进入、输出、和转发的分组，防火墙/网关和内部 LAN 用户之间的通信就无法进行。要允许用户执行与网络相关的功能以及使用联网应用程序，管理员必须打开某些端口进行通信。

例如：要允许到防火墙上的端口 80 的通信，添加以下规则：

```
iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT

iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

这会允许用户浏览通过端口 80 通信的网站。要允许到安全网站（如 https://www.example.com/）的访问，你还必须打开端口 443。

```
iptables -A INPUT -p tcp -m tcp --sport 443 -j ACCEPT

iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

有时候，可能会需要从 LAN 之外远程地进入 LAN。SSH 之类的安全服务可以用于到 LAN 服务的加密远程连接。对于拥有基于 PPP 资源的管理员来说，拨号进入可以被用来避开防火墙，因为调制解调器连接是直接连接，通常位于防火墙/网关之后。对于有宽带连接的远程用户来说，就需要制定些特殊规定。可以配置 iptables 接受来自远程 SSH 客户的连接。例如，要允许远程 SSH 访问，你可以使用以下规则：

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -p udp --sport 22 -j ACCEPT
```

这些规则允许个体系统的流量出入，如单个 PC 直接连接到互联网或防火墙/网关；然而，它们并不允许防火墙/网关之后的机器使用这些服务。要

允许 LAN 使用这些服务，可以使用带有 iptables 过滤规则的 NAT。

4.8.4 FORWARD 和 NAT 规则

多数机构从它们的 ISP 处得到数量有限的可公开选路的 IP 地址。鉴于这种限额，管理员必须积极寻求分享互联网服务的方法，而又不必把稀有的 IP 地址分配给 LAN 上的每一台机器。使用专用 IP 地址是允许 LAN 上的所有机器正确使用内部和外部网络服务的常用方法。网关可以接收来自互联网的通信，并把这些分组路由发送到它期望发送的 LAN 节点上；同时，防火墙/网关还可以把来自 LAN 节点的输出请求路由发送到远程互联网服务中。这种转发有时会很危险，特别是随着能够假冒内部 IP 地址、使远程攻击者的机器成为你的 LAN 上的一个节点的现代攻击工具的出现。为防止此类事件的发生，iptables 提供了路由发送和转发策略，你可以实施它们来防止对网络资源的欺诈利用。

FORWARD 政策允许管理员控制分组可以被路由发送到 LAN 内的哪些地方。例如：要允许整个 LAN 的转发（假定防火墙/网关在 eth1 上有一个内部 IP 地址），可以设置以下规则：

```
iptables -A FORWARD -i eth1 -j ACCEPT

iptables -A FORWARD -o eth1 -j ACCEPT
```

该规则允许防火墙/网关之后的系统能够进入内部网络。网关把 LAN 节点的分组路由发送到它的目的地，通过 eth1 设备传递所有分组。

接受通过防火墙的内部 IP 设备来转发的分组会允许 LAN 节点彼此通信；不过，它们没有被允许和外界（如互联网）通信。要允许带有内部 IP 地址的 LAN 节点和外部的公共网络通信，需要配置防火墙的 IP 伪装（IP masquerading）。这会把来自 LAN 节点的请求都伪装成防火墙的外部设备（在这个例子中是 eth0）的 IP 地址。

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

该规则使用 NAT 分组匹配表（-t nat），并在防火墙的外部联网设备（-o eth0）上为 NAT 指定内建的 POSTROUTING 链（-A POSTROUTING）。

POSTROUTING 允许分组在离开防火墙的外部设备时被改变。-j MASQUERADE 目标被用来使用防火墙/网关的外部 IP 地址来掩盖节点的内部 IP 地址。

如果你想让内部网络内的某个服务器能够被外部利用，你可以使用 NAT 内 PREROUTING 链的 -j DNAT 目标来指定该向哪个目标 IP 地址以及端口转发请求连接到内部服务的分组。例如，如果你想把进入的 HTTP 请求转发到 172.31.0.23 上的专用 Apache HTTP 服务器服务器系统，运行以下命令：

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \
      --to 172.31.0.23:80
```

该规则指定 NAT 表使用内建的 PREROUTING 链来仅把进入的 HTTP 请求转发到被列出的 IP 地址 172.31.0.23。

4.8.5 病毒和假冒 IP 地址

另外，可以限制某些类似特洛伊木马、蠕虫、以及其它客户/服务器病毒的可疑服务与它们的服务器连接。例如：有些特洛伊木马会扫描端口 31337 到 31340（即黑客语言中的 elite 端口）上的服务。阻塞这些端口能够有效地减少网络可能被感染的机器和它们的远程主服务器进行独立通信的机会。

```
iptables -A OUTPUT -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP
iptables -A FORWARD -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP
```

还可以阻塞试图假冒所在 LAN 的专用 IP 地址混入的连接。例如：LAN 使用 192.168.1.0/24 范围，面向互联网的网络设备（如 eth0）上就可以设置一条规则来丢弃到那个设备的使用你所在 LAN 的 IP 范围的分组。因为推荐使用的默认政策是拒绝转发分组，所有到面向外界的设备（eth0）的假冒 IP 地址都会被自动拒绝。

```
iptables -A FORWARD -s 192.168.1.0/24 -i eth0 -j DROP
```

4.8.6 iptables 和连接跟踪

iptables 包括一个模块，它允许管理员使用"连接跟踪"（connection tracking）方法来检查和限制到内部网络中可用服务的连接。连接跟踪把所有连接都保存在一个表格内，它令管理员能够根据以下连接状态来允许或拒绝连接：

- NEW —— 请求新连接的分组，如 HTTP 请求。
- ESTABLISHED —— 属于当前连接的一部分的分组。
- RELATED —— 请求新连接的分组，但是它也是当前连接的一部分，如消极 FTP 连接，其连接端口是 20，但是其传输端口却是 1024 以上的未使用端口。
- INVALID —— 不属于连接跟踪表内任何连接的分组。

可以和任何网络协议一起使用 iptables 连接跟踪的状态功能，即便协议本身可能是无状态的（如 UDP）。下面的例子显示的规则使用连接跟踪来只转发与已建立连接相关的分组：

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ALLOW
```

4.8.7 ip6tables

下一代互联网协议 IPv6 的出现突破了 IPv4（或 IP）的 32 位地址限制。IPv6 支持 128 位地址，因此识别 IPv6 的载体网络就能够制定比 IPv4 更多的可选路地址。

GTES10 支持使用 Netfilter 6 子系统和 ip6tables 命令的 IPv6 防火墙规则。使用 ip6tables 的第一步是启动 ip6tables 服务。它可以使用以下命令进行：

```
service ip6tables start
```

要使 ip6tables 在系统引导时默认启动，使用 chkconfig 来改变服务的运行级别状态。

```
chkconfig --level 345 ip6tables on
```

其语法在各方面都和 iptables 相同，只是 ip6tables 支持 128 位的地址。例如：在识别 IPv6 的网络服务器器上的 SSH 连接可以使用以下规则来启用：

```
ip6tables -A INPUT -i eth0 -p tcp -s 3ffe:ffff:100::1/128 --dport 22 -j ACCEPT
```

关于 IPv6 联网的详情，请参阅 IPv6 的信息页：http://www.ipv6.org/。

4.9 漏洞测定

该部分提供了对安全评估的理论和操作。

没有绝对安全的系统。路由器有助于保护通向互联网的网关的安全性；防火墙有助于保护网络边缘地带的安全性；虚拟专用网能够在加密流中安全地传递数据；入侵检测系统能够在出现蓄意活动时向你发出警告。然而，以上技术的成功与否都依赖诸多因素，这些因素包括：

- 负责配置、监视和维护相关技术的职员的专业程度。
- 进行快速有效地更新或给服务和内核打补丁的能力。
- 负责时刻警戒网络动静的职员的能力。

数据系统和技术的动态性使得保护企业资源的变得相当复杂。这种复杂性又给寻求各方面的系统专家带来一定难度。这主要是因为信息安全的每一领域都要求其专业人士全身投入和时刻关注。而且信息安全本身也不是一成不变的行业。

4.9.1 测定和测试

漏洞测定可以被分化成两类："由外向里看"（Outside looking in）和"由里向外看"（inside looking around）。

在进行"由外向里看"的漏洞测定时，是在试图从外部进入你的系统。站在系统之外会提供一个怪客的视角。会看到怪客所见 —— 可公开选路的 IP 地址、位于 DMZ 上的系统、整个防火墙的外在界面等等。DMZ 代表"停火区域"。它是指位于可信任的内部网络（如公司专用网）和不可信任的

外部网络（如公共互联网）之间的计算机或小型子网。典型的 DMZ 包括可被互联网交通进入的设备，如万维网（HTTP）服务器、FTP 服务器、电子邮件（SMTP）服务器和 DNS 服务器。

在进行"由里向外看"的漏洞测定时，是在系统上登录后的视角。会看到打印服务器、文件服务器、数据库、以及其它资源。

这两类漏洞测定截然不同。站在局内人的角度提供更多特权。然而，现在的多数机构中，安全配置的目的仍是旨在把入侵者拒之门外。在保持机构内部安全方面（如部门间的防火墙、用户级别的安全控制、内部资源的验证手续、等等）做的却相当少。通常，如果从内部看，可用资源要比从外部看要多，因为多数系统都是公司内部使用的。一旦你在公司之外，你就会被立即给予不信任级别。你可以使用的系统资源就会大受限制。

考虑一下漏洞测定和入侵测试（penetration tests）的区别。漏洞测定应该是入侵测试的第一步。测定中所积累的信息将会用于测试。漏洞测定是检查漏洞及潜在缺陷的过程，而入侵测试是试图利用这些漏洞缺陷的实践行为。

测定网络体系是一个动态过程。信息安全和物理安全都是动态的。执行测定只会显示一个大概，它有可能会造成一些假象，让你白担心或者空欢喜一场。

安全管理员只能尽其工具和知识经验之能。使用任何当前可用的测定工具，在系统上运行它们，几乎可以肯定会出现一些假警报。不管这是程序错误还是使用错误， 其结果都是一样的。工具可能会发现实际上不存在的漏洞（false positive）；同样，也可能漏掉实际上存在的漏洞（false negative）。

以下列表讨论了执行漏洞测定会带来的优势。

- 积极地将注意力集中到信息安全上
- 在怪客找到潜在漏洞前发现它们
- 通常导致系统的时刻更新和补丁的及时应用
- 鼓励成长，并有助于职员深化其专业知识
- 减少财政损失和消极宣传

4.9.2 评估工具

典型的测定可以从收集信息开始。在测定整个网络时，首先使用布局图来找出运行着的主机位置。逐个检查每台主机。

操作系统、应用程序、网络（根据使用协议而定）都有其特殊的测定工具。找到恰当的工具不是件轻而易举的事。说到底，经验最重要。如果可能，设立一个测试试验室，尽可能地多试一些工具，记录每个工具的强弱点。回顾工具的 README 文件或说明书页。此外，还可以在互联网上寻找更多信息，例如文章、指南、甚至专门讨论某个工具的邮件列表。

以下讨论的工具只是从可使用的大量工具中截取的一小部分。

4.9.2.1 使用 Nmap 来扫描主机

Nmap 被包括在 GTES10 中。Nmap 已经存在多年，可能是最常使用的收集信息工具，可以被用来判定网络布局。管理员可以在网络上使用 Nmap 来发现其中的主机和开放的端口。

Nmap 是比较合适的漏洞测定的第一步。可以用它测绘出网络内的所有主机的布局图，甚至传递选项来试图识别在某个主机上运行的操作系统。Nmap 为建立使用安全服务和禁用服务的策略奠定了良好基础。

4.9.2.1.1 使用 Nmap

Nmap 可以从 shell 提示下运行。在 shell 提示下，键入 nmap 命令，随后是要扫描的主机名或 IP 地址。

```
nmap foo.example.com
```

扫描的结果和以下类似：

```
Starting nmap V. 3.50 ( www.insecure.org/nmap/ )

Interesting ports on localhost.localdomain (127.0.0.1):

(The 1591 ports scanned but not shown below are in state: closed)
```

```
Port        State       Service
22/tcp      open        ssh
25/tcp      open        smtp
111/tcp     open        sunrpc
443/tcp     open        https
515/tcp     open        printer
950/tcp     open        oftep-rpc
6000/tcp    open        X11
Nmap run completed -- 1 IP address (1 host up) scanned in 71.825 seconds
```

Nmap 测试多数常用网络通信端口上的监听或等待服务。这些信息对于需要关闭的服务很有帮助。

关于使用 Nmap 的更多信息，请参阅以下 URL 上的官方网站：http://www.insecure.org/。

4.9.2.1.2 Nessus

Nessus 是一个功能完全的安全扫描器。Nessus 的插件体系允许用户为他们的系统和网络自行定制。和其它扫描器一样，Nessus 只能和它所依赖的签名数据库一样有效。它的功能包括：完整报告、主机扫描、真实时间的漏洞搜索。Nessus 也可能会出现假警报。Nessus 没有被包括在 GTES10 中，也不被支持。关于使用 Nessus 的更多信息，请参阅以下 URL 上的官方网站：http://www.nessus.org/。

4.9.2.1.3 Nikto

Nikto 是一个优秀的 CGI（公用网关接口）扫描器。Nikto 不仅具备检查 CGI 漏洞的能力。该程序还附带了良好的文档。在运行程序前应该仔细阅读文档。如果的万维网服务器提供 CGI 脚本，Nikto 是检查这些服务器安

全性的理想工具。Nikto 没有被包括在 GTES10 中，也不被支持。关于 Nikto 的更多信息，可以在以下 URL 上找到：http://www.cirt.net/code/nikto.shtml。

4.9.2.1.4 预先考虑将来需要

根据的目标和资源，可以使用的各种工具。这些工具有用于无线网络、Novell 网络的，也有用于 Windows 系统、Linux 系统的。执行测定的另一个重要部分可能会包括审核物理安全性、人员安全审查、或声音/PBX 网络测定。一些新的概念，如 war walking —— 扫描企业物理结构的边缘来寻找无线网络的可乘之机 —— 是你可以进行调查的新兴概念，若必要，可以包括在你的漏洞测定中。

4.10 入侵检测

恶意的用户和怪客会试图寻找较脆弱的目标，例如：未应用补丁的系统、被特洛伊木马病毒感染的系统、以及运行不安全服务的网络。管理员和安全组的成员在系统被攻击时应该收到警报，这样，他们才能够立刻对此类威胁做出相应的反应。入侵检测系统（Intrusion detection systems）就被设计成这样的警报系统。

4.10.1 入侵检测系统详述

入侵检测系统（IDS）是一种分析系统和网络上未经授权的进入和（或）有不良企图的活动的积极进程或设备。IDS 检测异常情况的方法可能会大相径庭；但是它们的最终目的都是在攻击者还未对你的系统造成损害前当场捕捉他们。

IDS 帮助系统免受攻击、滥用和弱化。它还能够监视网络活动、审查网络和系统配置中的漏洞、分析数据完好性等等。根据你选择要使用的检测方法而定，使用 IDS 有几种直接和间接的优越性。

4.10.1.1 IDS 类型

理解 IDS 的概念和它所提供的功能是判定哪种类型最适用于你的计算机安全政策的关键。本节讨论 IDS 的原理、各类 IDS 的功能、以及在一个软件包中使用多种检测技术和工具的合成 IDS 的出现。

某些 IDS 是知识性的（knowledge-based），它使用一个常见攻击的数据库在入侵发生前抢先警告安全管理员。此外，还有一些行为性（behavioral）的 IDS，它们跟踪所有异常资源使用，这些异常资源使用通常是蓄意破坏行为的标志。某些 IDS 是在后台运行的独立服务，只消极地监听活动，并记录来自外界的可疑分组。其它 IDS 综合使用标准的系统工具、改进的配置、详细的记录、以及管理员的直觉和经验，来创造一个强大的入侵检测工具包。试用并鉴定各类入侵检测技术能够帮助你找到 最适用于你所在机构的检测技术。

安全领域里最常见的 IDS 是基于主机（host-based）和基于网络（network-based） 的 IDS。基于主机的 IDS 是两者中最完整的一种。它在每个独立主机上布置一个监测系统。不管该主机位于哪个网络环境，它都被保护。基于网络的 IDS 在分组被发送给每个主机之前使其先被另一个设备过滤。它通常被认为是不太完整的监测方法，因为在可移环境中的许多主机都得不到可靠的网络分组过滤和保护。

4.10.2 基于主机的 IDS

基于主机（host-based） 的 IDS 分析几个方面来判定滥用（来自网络内部的蓄意或妄用活动）或入侵（来自外界的突破）情况。基于主机的 IDS 考查若干日志文件（内核、系统、服务器、网络、防火墙等等），并拿日志文件和常见已知攻击的内部数据库进行比较。UNIX 和 Linux 的基于主机的 IDS 大量使用 syslog 命令及其根据严重性来区分所要记录事件的能力。安装 sysklogd 软件包就可以使用 syslog 命令。该软件包被包括在 GTES10 。它提供了系统记录功能以及搜集内核消息功能。基于主机的 IDS 过滤日志（记录网络和内核事件的日志可能会非常详细）、分析日志、使用它自己的严重性级别系统来重新给异常消息标签、并把它们收集到它自己的特殊日志以供管理员分析使用。

基于主机的 IDS 还可以校验重要文件和可执行文件的完好性。它检查敏感文件（以及管理员添加的任何文件）的数据库，并使用 md5sum（128 位算法）或 sha1sum（160 位算法）之类的消息文件摘要工具来为每个文件创建一个校验和（checksum)。然后，基于主机的 IDS 把这些校验和保存到一个纯文本文件中，并定期比较实际文件的校验和与这个纯文本文件中保存的数值。如果发现了任何不匹配之处，IDS 就会通过电子邮件或传呼机来警告管理员。

4.10.2.1 Tripwire

Tripwire 是最流行的用于 Linux 的基于主机的 IDS。Tripwire, Inc. 是 Tripwire 的开发商，它们新近为 Linux 版本按照 GNU 通用公共许可证的条款开放了源码。ripwire 没有被包括在 GTES10 中，它也不被支持。Tripwire 在 http://www.tripwire.org/ 上可以获得。

4.10.2.2 RPM 作为一种 IDS

RPM 软件包管理器(RPM)是另一个可以被用作基于主机的 IDS 的程序。RPM 包含各类用于查询软件包及其内容的选项。对于那些怀疑重要的系统文件和可执行文件已被修改的管理员来说，这些校验选项具有很高的价值。

以下列表详细地描述了一些可以用来校验 GTES10 系统上的文件完好性的 RPM 选项。

- rpm -V 软件包名称

-V 选项校验已安装了的叫做"package_name"的软件包中的文件。如果该命令没有显示任何输出而退出，这就意味着其中所有文件自从最后一次 RPM 数据库更新以来都没有被修改。如果该命令给出了错误，例如：

```
S.5....T c /bin/ps
```

那么，这就说明该文件已被修改了。你需要决定是应该保留它（如果被修改的文件是 /etc 中的配置文件)还是删除它后再重新安装包含这个文件的软件包。以下列表解释了表示校验失败的这八个字符（上面例子中是

S.5....T）的含义。

. - 已通过这一阶段的校验测试

? - 测试中发现了一份无法读取的文件，这极可能是文件权限问题

S - 测试中发现了一份比最初安装在系统上的文件稍大或稍小的文件

5 - 测试中发现了一份和最初安装时的 md5 校验和不匹配的文件

M - 测试中检测到文件权限或文件类型错误

D - 测试中检测到主/次号码不匹配的设备文件

L - 测试中找到一个被改变到另一个文件路径的符号链接

U - 测试中找到一份用户所有者被改变的文件

G - 测试中找到一份组群所有者被改变的文件

T - 测试中遇到文件的 mtime 校验错误

- rpm -Va

-Va 选项校验所有安装了的软件包，并找出校验测试中的失败之处（和 -V 选项相似），但是由于它校验每个安装了的软件包，其输出要比 -V 选项更详细。

- rpm -Vf /bin/ls

-Vf 选项校验某个安装了的软件包中的单个文件。如果你打算只快速地校验一个有疑点的文件，这个选项就很有用。

- rpm -K application-1.0.i386.rpm

-K 选项对于检查 RPM 软件包文件的 md5 校验和与 GPG 签名来说很有用。你可以用它来检查你想安装的软件包是否被 Turbolinux 或被其它你已导入 GPG 公钥的机构签名了。没有被正确签名的软件包会显示一条和以下相似的消息：

```
application-1.0.i386.rpm (SHA1) DSA sha1 md5 (GPG) NOT OK (MISSING KEYS: GPG#897da07a)
```

在安装未被签名的软件包时请务必谨慎从事，因为它们没有被 Turbolinuxt,

Inc. 批准，有可能包含有害源码。

PRM 是一个强大的工具，它提供的诸多对安装软件包和 RPM 软件包文件的校验工具就足以证明这一点。我们建议你在安装了 GTES10 后，把 RPM 数据库目录（/var/lib/rpm/）备份到只读介质（如光盘）上，这样能够根据只读数据库而不是你的系统上的数据库来校验文件和软件包，因为有恶意的用户可能会破坏数据库来歪曲校验结果。

4.10.3 基于网络的 IDS

基于网络的入侵检测系统和基于主机的入侵检测系统的工作方式不同。基于网络的 IDS 的设计思想是在路由器或主机级别扫描网络分组、审查分组信息，并把可疑分组详细记录到一个特殊文件中。根据这些可疑分组，基于网络的 IDS 可以扫描它自己的已知网络攻击特征数据库，并为每个分组指定严重级别。如果严重级别够高，它就会给安全组的成员发送电子邮件或通知传呼机，因此安全组的成员就可以进一步调查这些异常情况的性质。

随着互联网在其范围和流量方面的增大，基于网络的 IDS 已经越来越受欢迎。在安全行业中，能够扫描大量网络活动并成功地标记可疑传输的 IDE 很受好评。鉴于 TCP/IP 协议所固有的安全问题，开发扫描器、嗅探器、以及其它网络评审和检测工具来防止由恶意的网络活动所带来的安全破坏已显得及其重要。这些活动包括：

- IP 假冒（Spoofing）
- "拒绝服务"攻击
- arp 缓存污染
- DNS 名称破坏
- 中间人攻击

多数基于网络的 IDS 需要把主机系统网络设备设置为混杂（promiscuous）模式。该模式允许设备捕捉每个经过网络的分组。混杂模式可以通过 ifconfig 命令来设置，例如：

```
ifconfig    eth0    promisc
```

运行不带选项的 ifconfig 会显示出 eth0 现在处于混杂（PROMISC）模式。

```
eth0    Link encap:Ethernet    HWaddr 00:00:D0:0D:00:01
        inet addr:192.168.1.50    Bcast:192.168.1.255    Mask:255.255.252.0
        UP BROADCAST RUNNING PROMISC MULTICAST    MTU:1500
        RX packets:6222015 errors:0 dropped:0 overruns:138 frame:0
        TX packets:5370458 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:2505498554 (2389.4 Mb)    TX bytes:152137517 (1450.8Mb)
        Interrupt:9 Base address:0xec80
lo
        Link encap:Local Loopback
        inet addr:127.0.0.1    Mask:255.0.0.0
        UP LOOPBACK RUNNING    MTU:16436    Metric:1
        RX packets:21621 errors:0 dropped:0 overruns:0 frame:0
        TX packets:21621 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:1070918 (1.0 Mb)    TX bytes:1070918 (1.0 Mb)
```

使用一个类似于 tcpdump 的工具，能够看到网络中的流量：

```
tcpdump: listening on eth0
02:05:53.702142 pinky.example.com.ha-cluster > \
   heavenly.example.com.860:    udp 92 (DF)
02:05:53.702294 heavenly.example.com.860 > \
 pinky.example.com.ha-cluster:    udp 32 (DF)
```

```
02:05:53.702360 pinky.example.com.55828 > dns1.example.com.domain: \
 PTR? 192.35.168.192.in-addr.arpa. (45) (DF)
02:05:53.702706 ns1.example.com.domain > pinky.example.com.55828: \
 6077 NXDomain* 0/1/0 (103) (DF)
02:05:53.886395 shadowman.example.com.netbios-ns > \
 172.16.59.255.netbios-ns: NBT UDP PACKET(137): QUERY; BROADCAST
02:05:54.103355 802.1d config c000.00:05:74:8c:a1:2b.8043 root \
 0001.00:d0:01:23:a5:2b pathcost 3004 age 1 max 20 hello 2 fdelay 15
02:05:54.636436 konsole.example.com.netbios-ns > 172.16.59.255.netbios-ns:\
NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
02:05:56.323715 pinky.example.com.1013 > heavenly.example.com.860:\
 udp 56 (DF)02:05:56.323882 heavenly.example.com.860 > pinky.\
  example.com.1013: udp 28 (DF)
```

可以看到，目的地不是本机的分组也会被 tcpdump 扫描并记录。

4.10.3.1 Snort

虽然 tcpdump 是一个很有用的评审工具，它并不是一个真正的 IDS，因为它并不分析或标记异常分组。tcpdump 把所有分组信息不加分析地打印到输出屏幕或日志文件中。一个正确的 IDS 将会分析分组、标记潜在的恶意分组传输、并把它贮存到一个格式化的日志中。

Snort 是一个 IDS，它能够准确简明地成功记录恶意网络活动，并在潜在破坏出现时通知管理员。Snort 使用标准的 libcap 库和 tcpdump 作为分组记录后端。

除了它的功能外，Snort 的最受重视的特性是其灵活的攻击特征子系统。Snort 有一个可以通过互联网来添加和更新的不断更新的攻击数据库。用户可以根据新网络攻击来创建其特征，并提交到 Snort 特征邮件列表中

（位于 http://www.snort.org/lists.html），因此所有的 Snort 用户都可以从中受益。这种社区共享精神使 Snort 成为最新最强健的基于网络的 IDS。Snort 没有被包括在 GTES10 中，它也不被支持，本书只是对它进行介绍。

4.11 恢复资源

要恢复系统，必须把所有终止的系统或程序重新启动，如验证服务器、数据库服务器。

建议你备有备份硬件，如额外的硬盘驱动器、热备份服务器等。备份系统应该安装了所有生产软件，能够被立即使用。这样，只有最近的和最相关的数据需要被导入。这个备份系统应该从可能会受影响的网络中隔离出来。

系统恢复是一项冗长而繁琐的工作。在许多情况下，有两种行动可选。管理员可以完整地重新安装操作系统，再恢复所有数据和应用程序。或者，管理员可以给出了问题的地方打补丁，然后再让受影响的系统重新回到生产环境中。

4.11.1 重新安装系统

执行完整的重新安装会确保受影响的系统中的所有"特洛伊木马"、后门、和恶意进程都被清除。重新安装还能够确保所有数据（如果从可信任的备份源中恢复了）都没有被恶意篡改。然而，完整的重新安装会花较长时间。如果有可用的热备份系统，只需要转储最近的数据，系统停运时间就会被大大缩短。

4.11.2 给系统打补丁

另一种恢复方法是给受影响的系统打补丁。这种方法执行起来比较危险，应该格外谨慎从事。其危险性取决于你是否已经完全地清除了系统内的"特洛伊木马"、漏洞和破坏性数据。如果使用的是模块化内核，那么给一个受损系统打补丁就更加困难。多数特洛伊木马系统命令、以及 shell 环境

被刻意设计用来从例行审核中隐藏入侵的行踪。

4.12 常见的漏洞攻击和常用的服务端口

该部分讨论了入侵系统或截取传输中数据的常用方法。还详细描述了一些最常使用的服务和相关端口号码。这些有助于减少系统被攻击。

4.12.1 常见的漏洞利用和攻击

表 4-3 详细列举了某些最常见的漏洞利用以及入侵者入侵的常用入口。避免这些常见漏洞被利用的关键是了解这些活动的方式。

漏洞利用	描述	备注
空白或默认口令	把管理性口令留为空白或使用产品生产商所设置的默认口令。虽然某些运行在 Linux 上的服务包含默认管理口令（GTES10 中并不包含），这种行为在硬件（如路由器和防火墙）中最常见。	在路由器、防火墙、VPN 和网络连接的贮存设备（NAS）中最常见。 在许多过时了的操作系统，特别是附带服务的 OS，如 UNIX 和 Windows 中也很常见。 管理员有时会在匆忙间创建一个有特权的用户而把口令留为空白。这就会成为发现了这个用户帐户的入侵者的完美入口。

漏洞利用	描述	备注
默认共享密钥	安全服务有时会把用于开发或评估测试目的的默认安全密钥打入软件包内。如果这些密钥不经改变而被用于互联网上的生产环境，那么*任何*拥有同样的默认密钥的用户都可以使用那个共享密钥资源，以及其中的保密信息。	在无线访问点和预配置的安全服务器设备中最常见。 CIPE 包含一个用于示范的静态密钥，在转入生产环境前，这个密钥必须被改变。
IP 假冒（Spoofing）	某个远程机器充当你的本地网络上的一个节点，它在你的服务器上寻找弱点，并安装一个后门程序或特洛伊木马来获取对你的网络资源的控制。	由于“假冒”要求怪客预测 TCP/IP SYN-ACK 号码来协调到目标系统的连接，它通常较难做到。但是有好几种工具可以帮助攻击者从事这类活动。 它倚赖于目标系统上运行使用*基于源*（source-based）的验证技术的服务（例如 rsh、telnet、FTP 等等）。和 PKI 及其它用在 ssh 或 SSL/TLS 的加密验证相比，这种验证技术是不被提倡的。

漏洞利用	描述	备注
窃听	通过窃听网络中的两个活跃节点的连接来收集它们之间传递的信息。	这类攻击多数在使用纯文本传输协议（如 Telnet、FTP、和 HTTP 传输）时发生。 远程攻击者必须具备到某个 LAN 上的一个已被弱化的系统的进入权；通常，该怪客已经使用了某种积极攻击方式（如 IP 假冒或中间人攻击）来弱化这个 LAN 上的某个系统。 防护措施包括加密钥匙、单次有效口令、以及防窃听的加密验证；强度加密传输也值得一试。

漏洞利用	描述	备注
服务弱点	攻击者在互联网上运行的某个服务中寻找缺陷或漏洞；通过这个弱点，攻击者可以危及整个系统以及系统上的任何数据，甚至还能够危及网络上的其它系统。	基于 HTTP 的服务，如 CGI，在执行远程命令甚至使用互动 shell 方面有弱点。即便作为一名无特权的用户来运行 HTTP 服务，攻击者也可以读取配置文件和网络图等。或者，攻击者可以发动“拒绝服务”攻击来用尽系统资源或使其无法为其他用户提供服务。 在开发和测试中，某些服务中的弱点可能没有被注意到；这些弱点（如：*缓冲区溢出*，buffer overflow。攻击者可以通过使用大于可接受的信息量来填充地址内存，导致服务崩溃，从而给攻击者提供一个互动命令提示。）能够给攻击者完全的管理控制。 管理员应该确保服务不是以根用户身份运行；并时刻关注来自开发商或安全组织（如 CERT 和 CVE）的补丁和勘误更新。
应用程序弱点	攻击者在桌面系统和工作站应用程序（如电子邮件客户程序）中寻找缺陷并执行任意程序编码、插入用于未来攻击行为的特洛伊木马、或者崩溃系统。如果被弱	工作站和桌面系统更容易被蓄意利用，因为使用工作站和桌面系统的用户没有防止或检测攻击活动的专业知识或经验。把安装未经授权的软件或打开不请自来的邮件的危险性通知给用户是极端重要的。

漏洞利用	描述	备注
	化的工作站拥有对整个网络的管理特权，还会发生进一步的漏洞利用。	可以实施一些防护措施，因此电子邮件客户软件不会自动打开或执行附件。此外，通过 Turbolinux 网络或其它系统管理服务来自动更新工作站软件也可以减轻应用多种安全政策所带来的负担。
拒绝服务（DoS）攻击	攻击者或一组攻击者通过给目标机器（服务器、路由器或工作站）发送未经授权的分组来协调对某个机构的网络或服务器资源的攻击。这会迫使合法用户无法使用资源。	在美国报导最多的 DoS 案例发生在 2000 年。那次攻击是一次协调的试通洪流（ping flood）攻击，它令几个带有高带宽连接的被弱化的系统成为僵尸（zombies），或重导向广播器，使好几家交通流量极大的商业和政府网站都陷于瘫痪。 源分组通常是伪造的（和重新广播的），这使调查攻击的真正发源地的任务变得很艰巨。 在使用 iptables 和类似 snort 的网络 IDS 技术的入口过滤（IETF rfc2267）方面的进展，给管理员跟踪并防御分布型 DoS 攻击提供了协助。

表 4-3. 常见漏洞利用

4.12.2 常用端口

下面的表格中列举了包括在 GTES10 中的服务、守护进程、和程序所使用的最常见的通信端口。该列表还可以在 /etc/services 文件中找到。要查看由互联网号码分派局（IANA）制定的"著名的已注册动态端口"官方列表，

请参考以下 URL：

http://www.iana.org/assignments/port-numbers

表 4-4 列举了被 IANA 定义的著名端口。它们被 GTES10 用作各类服务包括 FTP、SSH、和 Samba 的默认通讯端口。

端口号码 / 层	名称	注释
1	tcpmux	TCP 端口服务多路复用
5	rje	远程作业入口
7	echo	Echo 服务
9	discard	用于连接测试的空服务
11	systat	用于列举连接了的端口的系统状态
13	daytime	给请求主机发送日期和时间
17	qotd	给连接了的主机发送每日格言
18	msp	消息发送协议
19	chargen	字符生成服务；发送无止境的字符流
20	ftp-data	FTP 数据端口
21	ftp	文件传输协议（FTP）端口；有时被文件服务协议（FSP）使用
22	ssh	安全 Shell（SSH）服务
23	telnet	Telnet 服务
25	smtp	简单邮件传输协议（SMTP）
37	time	时间协议
39	rlp	资源定位协议
42	nameserver	互联网名称服务
43	nicname	WHOIS 目录服务

端口号码 / 层	名称	注释
49	tacacs	用于基于 TCP/IP 验证和访问的终端访问控制器访问控制系统
50	re-mail-ck	远程邮件检查协议
53	domain	域名服务（如 BIND）
63	whois++	WHOIS++，被扩展了的 WHOIS 服务
67	bootps	引导协议（BOOTP）服务；还被动态主机配置协议（DHCP）服务使用
68	bootpc	Bootstrap（BOOTP）客户；还被动态主机配置协议（DHCP）客户使用
69	tftp	小文件传输协议（TFTP）
70	gopher	Gopher 互联网文档搜寻和检索
71	netrjs-1	远程作业服务
72	netrjs-2	远程作业服务
73	netrjs-3	远程作业服务
73	netrjs-4	远程作业服务
79	finger	用于用户联系信息的 Finger 服务
80	http	用于万维网（WWW）服务的超文本传输协议（HTTP）
88	kerberos	Kerberos 网络验证系统
95	supdup	Telnet 协议扩展
101	hostname	SRI-NIC 机器上的主机名服务
102/tcp	iso-tsap	ISO 开发环境（ISODE）网络应用

端口号码 / 层	名称	注释
105	csnet-ns	邮箱名称服务器；也被 CSO 名称服务器使用
107	rtelnet	远程 Telnet
109	pop2	邮局协议版本 2
110	pop3	邮局协议版本 3
111	sunrpc	用于远程命令执行的远程过程调用（RPC）协议，被网络文件系统（NFS）使用
113	auth	验证和身份识别协议
115	sftp	安全文件传输协议（SFTP）服务
117	uucp-path	Unix 到 Unix 复制协议（UUCP）路径服务
119	nntp	用于 USENET 讨论系统的网络新闻传输协议（NNTP）
123	ntp	网络时间协议（NTP）
137	netbios-ns	在 GTES10 中被 Samba 使用的 NETBIOS 名称服务
138	netbios-dgm	在 GTES10 中被 Samba 使用的 NETBIOS 数据报服务
139	netbios-ssn	在 GTES10 中被 Samba 使用的 NETBIOS 会话服务
143	imap	互联网消息存取协议（IMAP）
161	snmp	简单网络管理协议（SNMP）
162	snmptrap	SNMP 的陷阱

端口号码 / 层	名称	注释
163	cmip-man	通用管理信息协议（CMIP）
164	cmip-agent	通用管理信息协议（CMIP）
174	mailq	MAILQ 电子邮件传输队列
177	xdmcp	X 显示管理器控制协议（XDMCP）
178	nextstep	NeXTStep 窗口服务器
179	bgp	边界网络协议
191	prospero	Prospero 分布式文件系统服务
194	irc	互联网中继聊天（IRC）
199	smux	SNMP UNIX 多路复用
201	at-rtmp	AppleTalk 选路
202	at-nbp	AppleTalk 名称绑定
204	at-echo	AppleTalk echo 服务
206	at-zis	AppleTalk 区块信息
209	qmtp	快速邮件传输协议（QMTP）
210	z39.50	NISO Z39.50 数据库
213	ipx	互联网络分组交换协议（IPX），被 Novell Netware 环境常用的数据报协议
220	imap3	互联网消息存取协议版本 3
245	link	LINK / 3-DNS iQuery 服务
347	fatserv	FATMEN 文件和磁带官吏服务器
363	rsvp_tunnel	RSVP 隧道

端口号码 / 层	名称	注释
369	rpc2portmap	Coda 文件系统端口映射器
370	codaauth2	Coda 文件系统验证服务
372	ulistproc	UNIX LISTSERV
389	ldap	轻型目录存取协议（LDAP）
427	svrloc	服务位置协议（SLP）
434	mobileip-agent	可移互联网协议（IP）代理
435	mobilip-mn	可移互联网协议（IP）管理器
443	https	安全超文本传输协议（HTTP）
444	snpp	小型网络分页协议
445	microsoft-ds	通过 TCP/IP 的服务器消息块（SMB）
464	kpasswd	Kerberos 口令和钥匙改换服务
468	photuris	Photuris 会话钥匙管理协议
487	saft	简单不对称文件传输（SAFT）协议
488	gss-http	用于 HTTP 的通用安全服务（GSS）
496	pim-rp-disc	用于协议独立的多址传播（PIM）服务的会合点发现（RP-DISC）
500	isakmp	互联网安全关联和钥匙管理协议（ISAKMP）
535	iiop	互联网内部对象请求代理协议（IIOP）
538	gdomap	GNUstep 分布式对象映射器（GDOMAP）

端口号码 / 层	名称	注释
546	dhcpv6-client	动态主机配置协议（DHCP）版本 6 客户
547	dhcpv6-server	动态主机配置协议（DHCP）版本 6 服务
554	rtsp	实时流播协议（RTSP）
563	nntps	通过安全套接字层的网络新闻传输协议（NNTPS）
565	whoami	whoami 用户 ID 列表
587	submission	邮件消息提交代理（MSA）
610	npmp-local	网络外设管理协议(NPMP)本地 / 分布式排队系统（DQS）
611	npmp-gui	网络外设管理协议（NPMP）GUI / 分布式排队系统（DQS）
612	hmmp-ind	HyperMedia 管理协议(HMMP)表示 / DQS
631	ipp	互联网打印协议（IPP）
636	ldaps	通过安全套接字层的轻型目录访问协议（LDAPS）
674	acap	应用程序配置存取协议（ACAP）
694	ha-cluster	用于带有高可用性的群集的心跳服务
749	kerberos-adm	Kerberos 版本 5(v5)的“kadmin”数据库管理
750	kerberos-iv	Kerberos 版本 4（v4）服务

端口号码 / 层	名称	注释
765	webster	网络词典
767	phonebook	网络电话簿
873	rsync	rsync 文件传输服务
992	telnets	通过安全套接字层的 Telnet（TelnetS）
993	imaps	通过安全套接字层的互联网消息存取协议（IMAPS）
994	ircs	通过安全套接字层的互联网中继聊天（IRCS）
995	pop3s	通过安全套接字层的邮局协议版本 3（POPS3）

表 4-4. 著名端口

表 4-5 列举了 UNIX 特有的端口。它包括了从电子邮件到验证等服务。包括在方括号内的名称（如 [service]）是服务的守护进程名称或常用别名。

端口号码 / 层	名称	注释
512/tcp	exec	用于对远程执行的进程进行验证
512/udp	biff [comsat]	异步邮件客户（biff）和服务（comsat）
513/tcp	login	远程登录（rlogin）
513/udp	who [whod]	whod 用户记录守护进程
514/tcp	shell [cmd]	无记录的远程 shell（rshell）和远程复制（rcp）

端口号码 / 层	名称	注释
514/udp	syslog	UNIX 系统日志服务
515	printer [spooler]	打印机（lpr）假脱机
517/udp	talk	Talk 远程对话服务和客户
518/udp	ntalk	网络交谈（ntalk），远程对话服务和客户
519	utime [unixtime]	UNIX 时间协议（utime）
520/tcp	efs	扩展文件名服务器（EFS）
520/udp	router [route, routed]	选路信息协议（RIP）
521	ripng	用于互联网协议版本 6（IPv6）的选路信息协议
525	timed [timeserver]	时间守护进程（timed）
526/tcp	tempo [newdate]	Tempo
530/tcp	courier [rpc]	Courier 远程过程调用（RPC）协议

端口号码 / 层	名称	注释
531/tcp	conference [chat]	互联网中继聊天
532	netnews	Netnews 新闻组服务
533/udp	netwall	用于紧急广播的 Netwall
540/tcp	uucp [uucpd]	UNIX-to-UNIX 复制服务
543/tcp	klogin	Kerberos 版本 5（v5）远程登录
544/tcp	kshell	Kerberos 版本 5（v5）远程 shell
548	afpovertcp	通过传输控制协议（TCP）的 Appletalk 文件编制协议（AFP）
556	remotefs [rfs_server, rfs]	Brunhoff 的远程文件系统（RFS）

表 4-5. UNIX 特有的端口

表 4-6 列举了由网络和软件社区向 IANA 提交的要在端口号码列表中正式注册的端口。

端口号码 / 层	名称	注释
1080	socks	SOCKS 网络应用程序代理服务
1236	bvcontrol [rmtcfg]	Gracilis Packeten 网络转换远程配置服务器 [a]
1300	h323hostcallsc	H.323 电讯主持电话安全

端口号码 / 层	名称	注释
1433	ms-sql-s	Microsoft SQL 服务器
1434	ms-sql-m	Microsoft SQL 监视器
1494	ica	Citrix ICA 客户
1512	wins	Microsoft Windows 互联网名称服务器
1524	ingreslock	Ingres 数据库管理系统（DBMS）锁定服务
1525	prospero-np	无特权的 Prospero
1645	datametrics [old-radius]	Datametrics / 从前的 radius 项目
1646	sa-msg-port [oldradacct]	sa-msg-port / 从前的 radacct 项目
1649	kermit	Kermit 文件传输和管理服务
1701	l2tp [l2f]	第 2 层隧道服务（LT2P） / 第 2 层转发（L2F）
1718	h323gatedisc	H.323 电讯守门装置发现机制
1719	h323gatestat	H.323 电讯守门装置状态
1720	h323hostcall	H.323 电讯主持电话设置
1758	tftp-mcast	小文件 FTP 组播
1759/udp	mtftp	组播小文件 FTP（MTFTP）
1789	hello	Hello 路由器通信端口
1812	radius	Radius 拨号验证和记帐服务
1813	radius-acct	Radius 记帐
1911	mtp	Starlight 网络多媒体传输协议（MTP）

端口号码 / 层	名称	注释
1985	hsrp	Cisco 热备用路由器协议
1986	licensedaemon	Cisco 许可管理守护进程
1997	gdp-port	Cisco 网关发现协议（GDP）
2049	nfs [nfsd]	网络文件系统（NFS）
2102	zephyr-srv	Zephyr 分布式即时消息服务器
2103	zephyr-clt	Zephyr 客户
2104	zephyr-hm	Zephyr 主机管理器
2401	cvspserver	并行版本系统（CVS）客户 / 服务器操作
2430/tcp	venus	用于 Coda 文件系统（codacon 端口）的 Venus 缓存管理器
2430/udp	venus	用于 Coda 文件系统（callback/wbc interface 界面）的 Venus 缓存管理器
2431/tcp	venus-se	Venus 传输控制协议（TCP）的副作用
2431/udp	venus-se	Venus 用户数据报协议（UDP）的副作用
2432/udp	codasrv	Coda 文件系统服务器端口
2433/tcp	codasrv-se	Coda 文件系统 TCP 副作用
2433/udp	codasrv-se	Coda 文件系统 UDP SFTP 副作用
2600	hpstgmgr [zebrasrv]	Zebra 选路
2601	discp-client [zebra]	discp 客户；Zebra 集成的 shell

端口号码 / 层	名称	注释
2602	discp-server [ripd]	discp 服务器；选路信息协议守护进程（ripd）
2603	servicemeter [ripngd]	服务计量；用于 IPv6 的 RIP 守护进程
2604	nsc-ccs [ospfd]	NSC CCS；开放式短路径优先守护进程（ospfd）
2605	nsc-posa	NSC POSA；边界网络协议守护进程（bgpd）
2606	netmon [ospf6d]	Dell Netmon；用于 IPv6 的 OSPF 守护进程（ospf6d）
2809	corbaloc	公共对象请求代理体系（CORBA）命名服务定位器
3130	icpv2	互联网缓存协议版本 2（v2）；被 Squid 代理缓存服务器使用
3306	mysql	MySQL 数据库服务
3346	trnsprntproxy	透明代理
4011	pxe	执行前环境（PXE）服务
4321	rwhois	远程 Whois（rwhois）服务
4444	krb524	Kerberos 版本 5（v5）到版本 4（v4）门票转换器
5002	rfe	无射频以太网（RFE）音频广播系统
5308	cfengine	配置引擎（Cfengine）
5999	cvsup [CVSup]	CVSup 文件传输和更新工具
6000/tcp	x11 [X]	X 窗口系统服务

端口号码 / 层	名称	注释
7000	afs3-fileserver	Andrew 文件系统（AFS）文件服务器
7001	afs3-callback	用于给缓存管理器回电的 AFS 端口
7002	afs3-prserver	AFS 用户和组群数据库
7003	afs3-vlserver	AFS 文件卷位置数据库
7004	afs3-kaserver	AFS Kerberos 验证服务
7005	afs3-volser	AFS 文件卷管理服务器
7006	afs3-errors	AFS 错误解释服务
7007	afs3-bos	AFS 基本监查进程
7008	afs3-update	AFS 服务器到服务器更新器
7009	afs3-rmtsys	AFS 远程缓存管理器服务
9876	sd	IP 多址传播会议的会话指挥
10080	amanda	高级 Maryland 自动网络磁盘归档器（Amanda）备份服务
11371	pgpkeyserver	良好隐私（PGP） / GNU 隐私卫士（GPG）公钥服务器
11720	h323callsigalt	H.323 调用信号交替
13720	bprd	Veritas NetBackup 请求守护进程（bprd）
13721	bpdbm	Veritas NetBackup 数据库管理器（bpdbm）
13722	bpjava-msvc	Veritas NetBackup Java / Microsoft Visual C++ (MSVC) 协议
13724	vnetd	Veritas 网络工具
13782	bpcd	Vertias NetBackup

端口号码 / 层	名称	注释
13783	vopied	Veritas VOPIE 验证守护进程
22273	wnn6 [wnn4]	假名/汉字转换系统
26000	quake	Quake（以及相关的）多人游戏服务器
26208	wnn6-ds	Wnn6 假名/汉字服务器
33434	traceroute	Traceroute 网络跟踪工具

注:

a. /etc/services 中的注释如下：端口 1236 被注册为“bvcontrol”，但是它也被 Gracilis Packeten 远程配置服务器使用。正式名称被列为主要名称，未注册的名称被列为别名。

b. 在 /etc/services 中的注释：端口 2600 到 2606 被 zebra 软件包未经注册而使用。主要名称是被注册的名称，被 zebra 使用的未注册名称被列为别名。

c. /etc/services 文件中的注释：该端口被注册为 wnn6，但是还在 FreeWnn 软件包中使用了未注册的“wnn4”。

表 4-6. 注册的端口

表 4-7 显示了一个和数据报传递协议（DDP）有关的端口列表。DDP 在 AppleTalk 网络上被使用。

端口号码 / 层	名称	注释
1/ddp	rtmp	路由表管理协议
2/ddp	nbp	名称绑定协议
4/ddp	echo	AppleTalk Echo 协议
6/ddp	zip	区块信息协议

表 4-7. 数据报传递协议端口

表 4-8 是和 Kerberos 网络验证协议相关的端口列表。在标记的地方，v5 代表 Kerberos 版本 5 协议。注意，这些端口没有在 IANA 注册。

端口号码 / 层	名称	注释
751	kerberos_master	Kerberos 验证
752	passwd_server	Kerberos 口令（kpasswd）服务器
754	krb5_prop	Kerberos v5 从属传播
760	krbupdate [kreg]	Kerberos 注册
1109	kpop	Kerberos 邮局协议（KPOP）
2053	knetd	Kerberos 多路分用器
2105	eklogin	Kerberos v5 加密的远程登录（rlogin）

表 4-8. Kerberos（工程 Athena/MIT）端口

表 4-9 是一个未注册的端口列表。这些端口可能被安装在你的 GTES10 系统上的服务或协议使用，或者它们是在 GTES10 和运行其它操作系统的机器通信所必需的端口。

端口号码 / 层	名称	注释
15/tcp	netstat	网络状态（netstat）
98/tcp	Linuxconf	Linuxconf Linux 管理工具
106	poppassd	邮局协议口令改变守护进程（POPPASSD）

端口号码 / 层	名称	注释
465/tcp	smtps	通过安全套接字层的简单邮件传输协议（SMTPS）
616/tcp	gii	使用网关的（选路守护进程）互动界面
808	omirr [omirrd]	联机镜像（Omirr）文件镜像服务
871/tcp	supfileserv	软件升级协议（SUP）服务器
901/tcp	swat	Samba 万维网管理工具（SWAT）
953	rndc	Berkeley 互联网名称域版本 9（BIND 9）远程配置工具
1127/tcp	supfiledbg	软件升级协议（SUP）调试
1178/tcp	skkserv	简单假名到汉字（SKK）日文输入服务器
1313/tcp	xtel	法国 Minitel 文本信息系统
1529/tcp	support [prmsd, gnatsd]	GNATS 错误跟踪系统
2003/tcp	cfinger	GNU finger
2150	ninstall	网络安装服务
2988	afbackup	afbackup 客户-服务器备份系统
3128/tcp	squid	Squid 万维网代理缓存

端口号码 / 层	名称	注释
3455	prsvp	RSVP 端口
5432	postgres	PostgreSQL 数据库
4557/tcp	fax	FAX 传输服务（旧服务）
4559/tcp	hylafax	HylaFAX 客户-服务器协议（新服务）
5232	sgi-dgl	SGI 分布式图形库
5354	noclog	NOCOL 网络操作中心记录守护进程（noclogd）
5355	hostmon	NOCOL 网络操作中心主机监视
5680/tcp	canna	Canna 日文字符输入界面
6010/tcp	x11-ssh-offset	安全 Shell（SSH）X11 转发偏移
6667	ircd	互联网中继聊天守护进程（ircd）
7100/tcp	xfs	X 字体服务器（XFS）
7666/tcp	tircproxy	Tircproxy IRC 代理服务
8008	http-alt	超文本传输协议（HTTP）的另一选择
8080	webcache	万维网（WWW）缓存服务
8081	tproxy	透明代理

端口号码 / 层	名称	注释
9100/tcp	jetdirect [laserjet, hplj]	Hewlett-Packard (HP) JetDirect 网络打印服务
9359	mandelspawn [mandelbrot]	用于 X 窗口系统的并行 mandelbrot 生成程序
10081	kamanda	使用 Kerberos 的 Amanda 备份服务
10082/tcp	amandaidx	Amanda 索引服务器
10083/tcp	amidxtape	Amanda 磁带服务器
20011	isdnlog	综合业务数字网（ISDN）记录系统
20012	vboxd	ISDN 音箱守护进程（vboxd）
22305/tcp	wnn4_Kr	kWnn 韩文输入系统
22289/tcp	wnn4_Cn	cWnn 中文输入系统
22321/tcp	wnn4_Tw	tWnn 中文输入系统（台湾）
24554	binkp	Binkley TCP/IP Fidonet 邮寄程序守护进程
27374	asp	地址搜索协议
60177	tfido	Ifmail FidoNet 兼容邮寄服务
60179	fido	默认 doNet 电子邮件和新闻网络

表 4-9. 未注册的端口

4.13 SELinux 介绍

本节是关于 SELinux 的简要介绍，在文中向你描述 SELinux 历史背景、体系构架及其安全策略概况等相关内容。

4.13.1 什么是 SELinux

SELinux，安全增强 Linux（Security-enhanced Linux），在内核里实现了强制访问控制（MAC），在通常 Linux 自主访问控制（DAC）后进一步进行访问检查，Selinux 主要包含一个安全构架（Flask 安全框架）和一系列安全策略（如：针对服务器的安全需求制定的 targeted 安全策略）。

4.13.2 SELinux 历史背景

SELinux 最早是由美国国防局（NSA）等资助开发的一个项目。它实现了 Flask 安全框架，实现了强制访问控制（MAC），提供可定制安全策略的能力，能根据系统中主体和客体对象的安全属性来实现安全规则。另外，Flask 框架还考虑了最小安全权限，它能提供一种机制让进程只能获得事先定义好的权限。

Flask 模型允许你用比较自然的语言来描述安全策略，这些安全规则的描述像使用一般句子一样。在这个模型中，允许你定义新的安全策略，并能重新运用之。在这个模型中还实现了 TE 和 RBAC 安全模型，为用户和应用程序提供透明的、更细致灵和的安全控制。

在新的 SELinux 版本中，NSA 使用 LSM 框架把 SELinux 集成到 linux 内核中。按照 Linus Torvlds 的建议，建立一个统一的安全框架框架（LSM）把包括 SELinux 在内其他安全模型也纳入其中。

最开始，SELinux 用 ext2 inode 中的一些域存储 PSIDS，这样就需要大量特殊的标识来描述安全属性，这样的实现方法需要修改每一个文件系统来支持并存储 PSIDS，这是一个伸缩性的很差的解决方案，不太能适应 Linux

内核的发展。

SELinux 在 2.4.<x>系列 Linux 内核使用可插入的 Linux 模块来实现，它采用普通的文件来存储 PSIDS，这样 SELinux 就能支持更多的文件系统。但是这种解决方案也不是最优的，在跨越平台的时候很容易造成不一致。现在 SElinux 集成到了主流的 2.6.x 内核代码树中，完全支持 LSM 并且使用文件系统 xattrs 特性接口来存储安全属性信息，这样安全模块和文件系统就可以相对独立，更容易进行扩展。

4.13.3 SELinux 目录和文件

SELinux 的 Flask 安全框架主要实现在 kernel 中，可以通过/selinux 文件系统进行访问和配置。

SELinux 的安全策略放在/etc/selinux/的两个目录:

- /etc/selinux/<policyname>/policy/ —— 二进制策略和运行时配置文件。
- /etc/selinux/<policyname>/src/policy/ —— 安全策略源码。

一个系统中存在多于一条策略是可能的，但是一次只能有一条被加载。策略的二进制文件，策略的原文件，存放在 /etc/selinux/<policyname>/，<policyname>是策略的名字，诸如 argeted、strict、webhost、test 等等。配置文件 /etc/selinux/config 定义了那个规则被使用，例如：SELINUXTYPE=targeted。

审计日志文件是一个重要文件。在 GTES10 中，这个可以由 /etc/syslog.conf 进行设置。

其他重要文件和目录包括 $SELINUX_POLICY/booleans 和 $SELINUX_POLICY/contexts/。SELinux 最重要的文件是二进制策略文件。这个文件存放在/etc/selinux/targeted/policy/policy.<XY>。<XY>是代表策略的两位数字。在 GTES10 中，这个文件是 policy.18。

4.13.4 SELinux 体系概览

在这节里是关于 SELinux 的体系结构的概览，主要讨论 SELinux 的安全策略、内核以及操作系统的其他部分是怎么联系在一起的。

4.13.4.1 Flask 安全体系和 SELinux

Flask 框架是为了解决传统 MAC 架构中几个遗留的问题而开发的，传统的 MAC 框架非常紧密的集成了多级访问控制模型（MLS），MLS 为每个主体定义了级别（clearances）,同时也为每个客体定义了类别（classifications），用于实现"上读"（read-up）和"下写"（write -down）。它提供了一个固定的规则让系统决定具有哪样安全级别的主体可以访问哪类别的客体。

这种不灵活的表现更多考虑的是数据的机密性，MLS 系统不关心数据完整性、最小安全权限和其他一些东西，它更关心系统上文件的机密性，确保未授权的用户不能访问到他们。

Flask 解决了这种不灵活性，通过把 policy enforement 从 policy logic 中分离出来，这部分被称为安全服务器。在传统的 Flask 中，安全服务器包含了安全策略逻辑，能够解释处理安全上下文。安全上下文或称为安全标签包含了一组进程或对象的安全属性。这些安全标签有这样的格式 <user>:<role>:<type>，例如： system_u:object_r:httpd_exec_t。SeLinux 用 system_u 来对 daemons 进行标识。使用 object_r 来表示如文件、设备这些系统对象这类角色。类型 httpd_exec_t 这个标识用于描述 httpd 能执行程序 /usr/sbin/httpd。

安全服务器只需要从主体-客体访问矩阵中查询相关的内容，并把这个结果保存在访问向量缓存中，以便下一次查询访问时候使用。

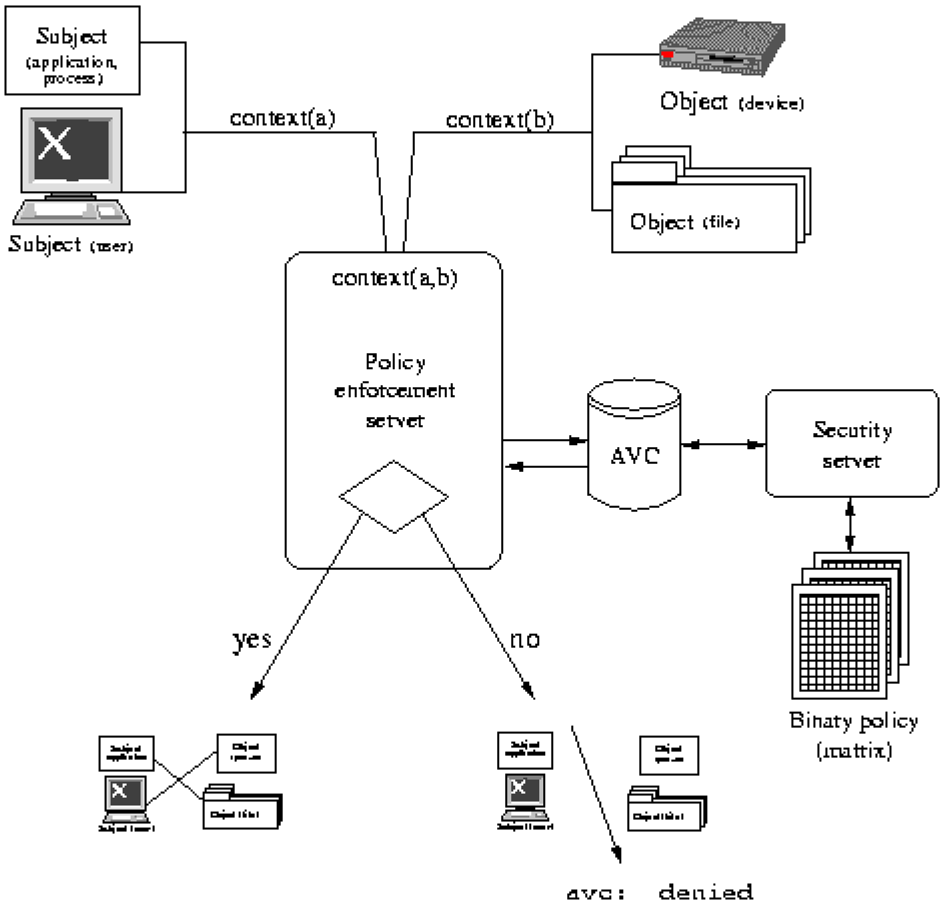


图 4-5 Flask 框架

图 4-5 描述了 Flask 框架，展示一个访问操作的全过程。在这个操作中，普通的自主访问控制（DAC）事先已经执行成功，然后再按照新的访问机制。

- 一个主体（比如说一个进程）试图去执行一个客体（比如说文件、设备、进程或者网络接口）。
- 策略执行服务器收集主体和客体的安全信息，并把这一对安全标签发送到安全服务器中，让它做出决定。

- 安全服务去首先检查 AVC，并把结果放回给策略执行服务器。如果在 AVC 中没有找到，就需要安全服务器根据在系统启动时候加载的二进制安全策略规则重新进行计算，并把它保存在 AVC 中。
- 如果安全策略允许该主体访问这个客体，这个操作就被允许执行。
- 如果策略不允许主体执行其期望的操作，操作就被拒绝：拒绝的消息写到$AUDIT_LOG 日志文件，在 GTES10 中，这个文件通常是/var/log/messages。

4.13.4.2 SELinux 是 Flask 框架的一种实现

SElinux 通过几次大的革新，最终被融合到 Linux 的内核。整个体系还是保持原样，但是很多实现细节已经改变。这些改变的原因包括：获得更广泛的接受的要求；LSM 的改变已经成为内核接受的一部分；用 xattrs 接口来存储 PSIDS 的需要。

作为内核版本变化的一个例子，原来的安全上下文通过将上下文映射到 SID 进行维持，通过安全服务器进行管理。在 Linux 2.6.内核中，文件的安全上下文存放在 xattrs 中，允许其保存自己的 SELinux 上下文。作为 Flask 体系的一个实现，SELinux 也被看作 LSM 的实现的一个参考。最初的 LSM 和 SELinux 以补丁的方式加到 2.4.<x>系列的内核；SELinux 不能作为一个可加载安全模块运行。

SELinux 开发团队的部分成员同时也在设计、开发和整合 LSM 到 Linux 内核。SELinux 的整合到内核，启动了 LSM 项目。SELinux 证明了 LSM 能够允许增强安全性被连接到内核，而不是嵌入在内核。最初，SELinux 是一个可加载模块，在内核 2.6.x 中，它被静态地编译到内核。SELinux 仍是一个 LSM 模块，它使用 LSM 在内核的钩子来控制和标记。因为抽象层同时被 LSM 和 Flask 构架支持,SELinux 具有高度的可配置性、可修改性。

Flask 足够灵活，能够工作在诸多不同的环境，而 Linux 天然就适合 Flask 模型。Linux 运行的平台的广泛性意味着 SELinux 已经被广泛测试。从长远来看，SELinux 整合到内核比使用可加载模块更容易获得成功。

同传统的 Flask 方法和最初的 SELinux 相比，以 SELinux 在 Linux 内核实

现 Flask 的方式具有以下的不同：

- 在传统的 TE 下，类型和域具有严格的区别。类型是文件对象的安全上下文，域是进程的安全上下文。在 SELinux 的实现中，两者没有实际的区别。在 SELinux 中，域是那些具有属性进程的进程，所以，术语域和传统的方式相同。同样，术语类型大多数应用于对象类型，但是，它既可指域也可以指类型。
- 由于透明性的原因，术语安全服务器仍旧实用，但是它已经不再是独立的服务。现在，安全服务器、AVC、策略引擎已经是内核的一部分。

4.13.5 SELinux 策略概览

本节概述 SELinux 安全策略，它内部一些特性，以及它的工作原理。

4.13.5.1 什么是策略

策略是规定 SELinux 安全引擎的规则的集合。策略定义了文件对象的类型和进程的域，使用角色来限制可进入的域，并且保持有用户的标志来制定可以获得的角色。当类型应用到进程的时候，类型和域是等同的。

类型是把具有安全相似性的对象归类的一种方法。例如，诸如文件这样的客体可以具有任何目的的任何上下文类型，但是如果它属于某个用户并且存放在用户的主目录，它就被当作属于特定的安全类型 user_home_t。

因为对于客体的类型，它们可以被相同的主体集合以同样的方式访问，因此，客体类型非常有用。同样，如果进程具有和其它客体相同的权限，这些进程趋于被认为是同样的类型。从 SELinux 的角度来看，这意味着进程被规定了什么能做，什么不能做。

策略定义了各种规则，以确定每个域可以访问的每一个类型。只有那些规则规定了许可的操作，才被允许执行。默认情况下，所有的操作被拒绝、审计，并被记录到文件$AUDIT_LOG,例如/var/log/messages。策略被编译成二进制格式，并被加载到内核安全服务器。

SELinux 以基于角色的限制的方式实现了“域-类型”的访问控制。策略规

定了相关环境下的规则。策略使用一种专用的简单语言进行书写。策略编写人员使用宏 m4 来获取通用的低级规则。现有的策略中有大量的 m4 宏，这些宏对于编写新的策略有极大的帮助。这些规则预处理的时候被处理成多条规则，成为 policy.conf 的一部分，policy.conf 最后被编译成二进制策略。

在$SELINUX_SRC/策略目录树中，文件被划分为各种不同的类型。访问权限被划分成不同的域。策略可以控制进入或切换域。

4.13.5.2 策略保存所在的位置

策略由两部分构成：二进制树和源码树。二进制树来自 selinux-policy-<policyname> 包，支持二进制策略文件。反之，当 selinux-policy-<policyname> —— sources 包安装了以后，二进制策略可以从源码编译而来。对于 GTES10 而言，<policyname>是 targeted。

- /etc/selinux/targeted/ —— 是 targeted 策略的根目录,包括二进制和源码树。

- /etc/selinux/targeted/policy/ —— 二进制策略文件 policy.<XY>存放在这里，变量$SELINUX_POLICY/用来表示该目录。

- /etc/selinux/targeted/src/policy/ —— 这是策略源码的存放地址。本指南中，$SELINUX_SRC/用来表示该目录。

- /etc/selinux/targeted/contexts/ —— 安全上下文信息和配置文件的存放目录，运行时被各种应用使用。改目录包括：

  #*_context* and efault_type —— 各种应用程序使用的上下文，例如 userhelper 使用的 userhelper_context。

  #files/* —— 文件 file_contexts 包括整个文件系统的默认上下文。 媒体文件包括了默认的诸如 CD-ROM 和软盘的媒体设备的默认上下文。

  #users/* —— 在 targeted 策略中，只有 root 文件在这个目录中。这些文件用来决定登陆的上下文。

- booleans —— 用来配置运行时 Booleans。当 Boolean 值发生改变的时

候，这是权威的配置文件。

应用需要各种不同的 SELinux 路径，libselinux 有大量的函数可以返回不同的配置文件和目录的路径。这样可以避免应用使用硬编码来指定路径。可以使用 man 3 selinux_binary_policy_path 来查看相关的函数。

4.13.5.3 策略在系统启动过程中的角色

SELinux 在系统初始化早期就扮演重要的角色。为了确保所有的进程都被标记正确的域，在启动过程中 init 程序执行了一些基本的操作，以确保进程被标记的安全属性和策略执行时保持一致。

- 在启动期间 kernel 被加载后，initial 进程被赋予 initial SID 的安全属性，该属性被用于在安全策略加载前的所做的启动工作。
- /sbin/init 挂载/proc，寻找是否存在 selinuxfs 文件系统，如果存在，就表示 kernel 中的 SELinux 特性是被允许的。
- 如果在 kernel 中没有发现 selinuxfs 文件系统，或者从启动参数中发现 selinux=0，或者从/etc/selinux/config 中发现 SELINUX=disabled，那么就启动一个没有 SElinux 特性的系统。

与此同时，init 进程为通过 kernel 启动参数 enforcing=0 或 enforcing=1 来更新配置文件/etc/selinux/config 中 enforcing 相应的值。

- 如果 SElinux 存在，/selinux 就被加载。
- init 进会根据/selinux/policyvers 和/etc/selinux/config 中 policy 的类型，决定装载那个的那个策略文件$SELINUX_POLICY/policy.<version>。
- 当安全策略加载后，初始的 SIDS 已经被定义，就像在$SELINUX_SRC/initial_sid_contexts 中定义的那样。
- 最后 init 继续剩下的启动工作。

4.13.5.4 什么是 Targeted 策略

SELinux 策略具有高度的可配置性。就 GTES10 而言，Turbolinux 支持一

种单独的策略 —— targeted 策略。在这个策略下，除非指定了 targeted 域，否则每一个主体和客体都运行在 unconfined_t 域。对于系统上域为 unconfined_t 的主体，SELinux 没有进行任何限制，使用标准的 Linux 安全，即 DAC。这个策略足够灵活，能够适应企业机构。守护进程是运行在它们域上的 targeted 策略的一部分，这些守护进程的操作被限制在被许可的范围之内。通过这种方式，守护进程的破坏性得到限制。

和 targeted 策略相对的是 strict 策略。strict 策略并没有在 GTES10 中发行。在 strict 策略中，每一主体和客体都在制定的安全域中，所有的相互操作和转换都被单独地在策略规则中考虑。strict 策略相对更复杂得多。

本指南主要讲解 GTES10 的 targeted 策略，以及 targeted 守护进程使用的 SELinux 组件。这些 targeted 守护进程包括：

- dhcpd
- httpd
- mysqld
- named
- nscd
- ntpd
- portmap
- postgres
- snmpd
- squid
- syslogd
- winbind

策略可以通过命令行或图形工具进行操纵。